TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

KYBERRISKIEN VAIKUTUS EUROOPAN KAUPALLISEN SIVIILI-ILMAILUN KYBERTURVALLISUUTEEN JA SÄÄNTELYYN

Vakuutustiede
Pro gradu -tutkielma
Joulukuu 2018
Tekijä: Eetu Aumala

Ohjaaja: Lasse Koskinen

TIIVISTELMÄ

Tampereen yliopisto	Johtamiskorkeakoulu: vakuutustiede
Tekijä:	AUMALA, EETU
Tutkielman nimi:	Kyberriskien vaikutus Euroopan kaupallisen siviili-ilmailun kyberturvallisuuteen ja sääntelyyn
Pro gradu -tutkielma:	88 sivua
Aika:	Joulukuu 2018
Avainsanat:	Siviili-ilmailu, kyberriski, sääntely, kyberuhka, kyberturvallisuus, ilmailuala, riskienhallinta

---

Laitteet ja teknologia ovat tuoneet merkittäviä hyötyjä ja mahdollisuuksia kaupalliselle siviili-ilmailulle. Hyötyjen lisäksi ne ovat altistaneet toimialan uusille riskeille, joita ei vielä täysin ymmärretä. Nämä riskit, joita kutsutaan kyberriskeiksi, ovat aiheuttaneet useita turvallisuuteen vaikuttavia tapahtumia viimeisen kahdenkymmenen vuoden aikana ja niiden määrän ennustetaan vain lisääntyvän entisestään. Kyberriskit voivat aiheuttaa merkittäviä taloudellisia tappioita, luottamuksen heikentymistä ja turvallisuusongelmia, minkä vuoksi niiden huomioiminen on elintärkeää kaupallisen siviili-ilmailun tulevaisuuden kannalta.

Tämän tutkimuksen tarkoituksena on selvittää mitä kaupallisen siviili-ilmailun kyberriskejä on tunnistettu alan tutkimuksissa ja miten tunnistetut kyberriskit vaikuttavat tai voivat vaikuttaa tällä hetkellä ja lähitulevaisuudessa kaupallisen siviili-ilmailun kyberturvallisuuteen. Tutkielma tutkii kyberriskien tunnistamista ja kyberturvallisuusvaikutusta systemaattisen kirjallisuuskatsauksen menetelmällä. Tämän lisäksi tutkielmassa selvitetään miten kyberriskit ovat vaikuttaneet Euroopan kaupallisen siviili-ilmailun sääntelykehitykseen tuoden esiin kriittisiä huomioita sääntelyn sisällöstä ja implementoinnista. Sääntelyn kartoitus on tehty narratiivisen kirjallisuuskatsauksen tutkimusmenetelmällä. Tutkielma on toteutettu laadullisin tutkimusmenetelmin aiheen tutkimattomuuden vuoksi. Kerättyä aineistoa analysoidaan tutkielmassa sisällönanalyysin keinoin.

Tutkielmassa havaittiin, että operationaalisista kyberriskeistä ihmisen toiminta vaikuttaa laajimmin siviili-ilmailun kyberturvallisuuteen, missä suurimpina uhkina ovat etä- ja lähihyökkäykset. Toiseksi suurin vaikutus on järjestelmähäiriöillä ja teknologisilla vioilla, jotka ovat hyökkäyksiä todennäköisempiä. Kolmanneksi suurin vaikutus on jaetusti ulkoisilla tapahtumilla ja epäonnistuneilla sisäisillä prosesseilla, joiden vaikutus pohjautuu paljolti kerroinvaikutuksiin kyberriskien vahvasti keskenään korreloivan luonteen vuoksi. Kyberriskit voivat vaikuttaa kyberturvallisuuteen aiheuttamalla onnettomuuksia, viivästymisiä, epäselviä tilanteita sekä luottamuksen menettämistä. Kyberriskien vakiintumattomuus voitiin havaita niin toimialan tutkimuksissa kuin sääntelyssäkin. Sääntelyn osalta tutkielmassa havaittiin uuden sääntelyn luomisen kiihtynyt tahti, joka osoittaa Euroopan sääntelijöiden keskittymisen ilmiöön. Sääntelystä tunnistettiin myös yleisluontoisuutta, mikä sysää vastuuta sääntelyä tulkitseville osapuolille ja heikentää sääntelyn luotettavuutta. Sääntelyn laajuuden havaittiin olevan mahdollinen ongelma kyberturvallisuuden takaamisen kannalta.

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Tutkielman taustaa

”Kyber” on terminä lisääntyvissä määrin osana elämäämme ja me hyväksymme sen olemassaolon usein passiivisesti. Ajoneuvot, laitteet, ohjaamot ja kodit ovat joko yhdistettyinä verkkoon tai verkon välityksellä toisiinsa. Laitteiden lisäksi yritykset, kuten kaupat ja vakuutusyhtiöt ovat verkottuneita. Vaikuttaa siltä, että kaikki on yhteydessä kaikkeen. (Ulsch 2014, xv–xvi) Laitteet ja teknologia tuovat mukanaan suuria hyötyjä ja mahdollisuuksia, mutta niiden kääntöpuolella on altistuminen merkittäville riskeille. Riskit, joille teknologia ja laitteet altistavat, ovat nimeltään kyberriskejä. (Institute of Risk Management 2014, 7–8)

Kyberriski on verrattain uusi riski, minkä vuoksi organisaatioiden tietämys riskistä on usein vajavaista, eikä moni organisaatio osaa käsitellä kyberriskiä. Teknologian yleistymisen vuoksi riski koskettaa kuitenkin kaikkia, niin suuria kuin pieniä toimijoita. (Institute of Risk Management 2014, 10) Kyberriskien vuosikustannusta on vaikea arvioida tarkasti. Yleisesti ottaen arviot päätyvät yli 100 miljardin dollarin vuosittaisiin kustannuksiin, tehden riskistä erittäin merkittävän. Kyberriskit voivat korreloida hyvin vahvasti toistensa kanssa lisäten riskiä, eikä niillä tunnu olevan kansallisia tai muita maantieteellisiä rajoja teknologian globaalin olemuksen vuoksi. (Eling & Schnell 2016, 477)

Siviili-ilmailun toimijat luottavat kasvavissa määrin teknologiaan toiminnassaan. Teknologiaan luottaminen kriittisissä operatiivisissa toimissa avaa kuitenkin ovia merkittäville kyberhyökkäyksille ja muille kyberuhkille, jotka ovat nousseet kriittiseksi huolenaiheeksi siviili-ilmailusta vastaaville tahoille. (ICAO 2018a) Euroopan lentoturvallisuusviraston mukaan siviili-ilmailu on houkutteleva kohde kyberhyökkäyksille, minkä vuoksi virasto haluaa varmistaa että kyberriskit ovat huomioitu lentokoneiden suunnittelussa, kehityksessä ja operoinnissa. Erityisen tärkeänä Euroopan siviili-ilmailuun liittyvien kyberriskien käsittelyssä pidetään riskien torjumista ja kansalaisten turvallisuutta. (EASA 2018a)

Kaupallisella siviili-ilmailulla tarkoitetaan ilmailutoimintaa, jossa kuljetetaan rahtia tai henkilöitä maksua vastaan. (IAOPA 2018) Kaupallinen siviili-ilmailu on kasvanut yhdistämään koko

maailmaa matkustamisen kautta. Se kuljettaa tällä hetkellä enemmän rahtia ja matkustajia nopeammin kuin ikinä ennen. Kyberriskille erityisen alttiin alasta tekee sen teknologiakeskeisyys. Ilmailualalla erityisesti keskiössä ovat ohjelmistot, verkostot ja laitteistot. Matkustajat käyttävät teknologiaa aina matkojen varaamisesta lennon aikana käytettävään langattomaan verkkoon asti. Lentokoneet sisältävät teknologiaa joka osa-alueellaan autopilotista navigointi- ja radioteknologiaan. Teknologioiden avulla pidetään myös yhteyttä lennonjohtoon. Kyberriski on siis läsnä ilmailussa lentokentillä, lennonjohdossa ja lentokoneissa, niin maasta käsin toimiessa kuin ilmassakin. (Haass, Sampigethaya & Capezzuto 2016, 39–41)

Kyberriskien potentiaalinen mahdollisuus vaikuttaa toimialaan piilee siinä, että riski on verrattain uusi ja teknologian kehittyessä uusia riskejä ilmenee alalla aikaisempaa tiheämmin (Haass ym. 2016, 39). Toimialalla riski on selvästi huomattu, sillä PricewaterhouseCoopersin (2016, 3) tekemän kyselyn mukaan lentoyhtiöiden toimitusjohtajista 85 % oli huolissaan kyberriskistä, kun taas muiden alojen toimitusjohtajien vastaava luku oli 61 %. Kaupallisen siviili-ilmailun ekosysteemi koostuu järjestelmien verkostosta, jossa lentokoneet ja niiden käyttäjät ovat yhteydessä keskenään kilpailevien lentoyhtiöiden ja lentokenttien järjestelmiin, kansallisiin lennonjohtojärjestelmiin, henkilöstöön ja matkustajiin. Järjestelmät ovat näin ollen hyvin verkottuneita keskenään. Kyberuhkat voivat heikentää toimialan turvallisuutta vaikuttamalla ekosysteemin kriittisiin infrastruktuureihin. Ilmailualan näkyvyys ja laaja skaala tekevät alasta erityisen alttiin kyberriskeille ja hyökkäyksille. (Haass ym. 2016, 40)

Yksi ensimmäisistä toteutuneista kyberriskeistä ilmailualalla oli vuonna 1997 tapahtunut palvelunestohyökkäys Yhdysvalloissa, jossa hyökkääjä hyödynsi paikallisen lentokentän tietoliikenneverkon haavoittuvuutta. Hyökkäyksen toteutti teini-ikäinen hakkeri. (Haass ym. 2016, 40) Hyökkäys poisti käytöstä lentokentällä olleen puhelinyhtiön tietokoneen kuudeksi tunniksi. Tietokoneen avulla ylläpidettiin yhteyksiä maan ilmailuviranomaiseen, lennonjohtotorniin, lentokentän palokuntaan, turvallisuusosastoon ja sääpalveluihin. Hyökkäys esti yhteydenpidon kuudeksi tunniksi aiheuttaen turvallisuusuhkan ja taloudellisia tappioita lentokentälle. (Cruz-Cunha & Portela 2015, 10) Lentokenttien kyberhyökkäyksiä on lähiaikoina kohdistettu kasvavissa määrin lentokenttien passitarkastukseen, henkilöstöön, matkustajiin ja matkatavaroiden hallintaan (Haass ym. 2016, 40).

Vuonna 2012 ongelmat satelliittipaikannusjärjestelmä GPS:n toimivuudessa häiritsivät Yhdysvalloissa Liberty International lentokentän toimintaa. Häiriöiden syyksi paljastui rekan kuljettaja, jolla oli käytössään GPS-järjestelmän häirintälaite, jotta työnantaja ei saisi tietää hänen sijaintiaan. GPS-järjestelmän osalta on lisäksi vuodesta 2013 vuoteen 2016 ilmoitettu noin 80 tapausta, jossa järjestelmä on antanut joko väärän sijainnin tai ei ole toiminut ollenkaan. (Kessler & Craiger 2018, 15–16)

Vuonna 2013 yli 75 lentokenttää Yhdysvalloissa raportoivat kalastelusähköposteista, joilla yritettiin huijata vastaanottajia paljastamaan maksutietojaan. Miamin kansainvälinen lentokenttä raportoi samana vuonna vastaanottavansa yli 20 000 hakkerointiyritystä joka päivä. Los Angelesin kansainvälinen lentokenttä puolestaan esti yli 60 000 lentokentän verkkosivuihin kohdistuvaa väärinkäytöksen yritystä sekä 2,9 miljoonaa hakkerointiyritystä. Kesäkuussa vuonna 2014 Itävallan, Tšekin, Saksan ja Slovakian lennonjohdot ilmoittivat useiden lentojen kadonneen näkyvistä kuuden päivän ajanjaksolla. Tutkasta katoamisten syyksi epäiltiin lähistöllä tapahtunutta armeijan toteuttamaa sähköisen sodankäynnin harjoitusta. (Haass ym. 2016, 40)

Vuonna 2015 Puolan kansallinen lentoyhtiö LOT joutui kyberhyökkäyksen kohteeksi. Hyökkäys poisti käytöstä lähtevien lentokoneiden lentosuunnitelmat, mikä aiheutti Varsovan kentältä lähtevien yhtiön lentojen ohjaamisen takaisin kentälle. Hyökkäyksen vuoksi kymmenen lentokonetta asetettiin lentokieltoon ongelman selvittämisen ajaksi. Vastaava lentosuunnitelmat poistava hyökkäys Yhdysvalloissa aiheutti samana vuonna kaikkien lentoyhtiö United Airlinesin lentokoneiden ohjaamisen takaisin kentälle. Lentokoneet asetettiin lentokieltoon ongelman selvittämisen ajaksi. Myös Ruotsin ilmatila kärsi vuonna 2015 kyberhyökkäyksestä, kun venäläinen hakkeriryhmä jumitti lennonjohdon välineistöä aiheuttaen satojen lentojen ohjaamisen takaisin lentokentälle viiden päivän ajanjaksolla. (Kessler & Craiger 2018, 8, 11; Haass ym. 2016, 40)

Vuonna 2016 Yhdysvalloissa Department of Homeland Securityn suorittama koe johti onnistuneeseen etänä toteutettuun järjestelmiin tunkeutumiseen Boeingin 757-malliseen lentokoneeseen. Kokeessa ei käytetty apuna yhteistyötä lentokoneen sisältä. Kokeessa käytettiin vain materiaaleja, joita oli mahdollista viedä turvallisuustarkastuksesta läpi. Boeing kiisti lentoko-

neen lentojärjestelmien vaarantumisen kokeen johdosta. (Kessler & Craiger 2018, 9) Vietnamin lentokenttiin kohdistettiin vuonna 2016 hyökkäyksiä aiheuttaen sähköisten lähtöselvitysten hetkellisen alasajon. Hyökkäyksellä uudelleenohjattiin myös Vietnam Airlines -lentoyhtiön verkkosivulla asioivat asiakkaat hyökkääjien asettamille ulkomaisille verkkosivuille. Yhtiön asiakkaiden tietoja vuodettiin myös verkkoon. (ENISA 2016)

Vuonna 2017 Yhdysvaltalaisen Virgin America -lentoyhtiön järjestelmiin murtauduttiin aiheuttaen työntekijöiden kirjautumistietojen ja henkilökohtaisten tietojen, kuten sosiaaliturvatunnusten, ajokorttien, osoitteiden ja nimien, altistumisen. Tapahtumien vuoksi yhtiö määräsi työntekijänsä muuttamaan salasanansa ja tarjosi vuoden ilmaisen identiteettivarkauden vastaisen palvelun ulkoiselta palveluntuottajalta hyökkäyksen kohteeksi joutuneille työntekijöilleen. Yhtiö kertoi muuttaneensa järjestelmiään hyökkäyksen johdosta sekä asettaneensa turvallisuusprotokollansa ja toimintatapansa tarkastukseen. Yhtiö ei raportin mukaan tehnyt hyökkäyksen myötä laajempia muutoksia toimintaansa. (Department of Justice 2017) Vuonna 2018 Yhdysvaltalainen lentoyhtiö Delta Airlines sai tiedon chat-palveluntoimittajaltaan, joka ilmoitti palveluntoimittajan altistuneen kyberhyökkäykselle. Hyökkääjät saattoivat saada hyökkäyksen kautta palvelusta ostonsa tehneiden asiakkaiden maksutietoja. Delta tarjosi tämän johdosta asiakkailleen ilmaisen luottovalvonnan työkalun. (Delta 2018)

Vuonna 2017 haittaohjelmat WannaCry ja Petya vaikuttivat muun muassa Ukrainan Boryspil-lentokentän tietokoneisiin. Myös lentokonevalmistaja Boeingin tietokoneet kärsivät haittaohjelmasta. Ohjelmat salaavat saastuneen tietokoneen tiedostot ja vaativat käyttäjältä maksua tiedostojen vapauttamiseksi. Saastunut tietokone saattaa levittää haittaohjelman tietokoneisiin, joihin se on yhteydessä. Maailmanlaajuisesti pelkästään WannaCry-kiristyshaittaohjelma vaikutti vuoden 2017 aikana ainakin 200 000 tietokoneeseen yli 150 maassa. WannaCryn ja Petyan yhteenlasketut kustannukset saattavat ylittää 4 miljardia dollaria maailmanlaajuisesti. (Kessler & Craiger 2018, 22)

Edellä esitellyt tapaukset ovat julkisesti esille tulleita. Näiden lisäksi voidaan epäillä olevan useita kyberhyökkäyksiä ja kybertapahtumia, joista ei ole kerrottu julkisuuteen. Huomattavaa on, että kyberhyökkäyksiä on kaupallisessa siviili-ilmailussa koettu vasta noin 20 vuoden ajan. Tänä aikana vuosittaisten hyökkäysten määrä on kasvanut merkittävästi. Erityisesti lähivuosina kyberhyökkäykset ovat yleistyneet tehden kyberriskeistä kaupallisessa siviili-ilmailussa

hyvin ajankohtaisen aiheen. Kaupallinen siviili-ilmailu on nykyisessä laajuudessaan hyvin paljolti teknologiaan luottava ja teknologian mahdollistama ala. Tämän vuoksi kyberriskien tutkiminen alan osalta on tarpeellista.

1.2 Tutkielman tavoitteet, tutkimusongelmat ja rajaukset

Tutkielman tavoitteena on kartoittaa kaupalliselle siviili-ilmailulle merkittäviä kyberriskejä ja niiden sääntelyä tällä hetkellä sekä lähitulevaisuudessa. Kaupallisen siviili-ilmailun kyberriskejä kartoitetaan maailmanlaajuisesti niiden globaalin ja rajattoman luonteen vuoksi. Kyberriskeihin liittyvää sääntelyä tarkastellaan Euroopan tasolla sääntelyn maakohtaisten eroavaisuuksien ja laajuuden vuoksi. Kartoituksen lisäksi tutkielmassa tutkitaan kyberriskien vaikutusta kaupallisen siviili-ilmailun sääntelyn muodostumiseen.

Tutkielma pyrkii vastaamaan kahteen tutkimusongelmaan, jotka ovat:

> *1) Miten kyberriskit voivat vaikuttaa kaupallisen siviili-ilmailun kyberturvallisuuteen?*
>
> *2) Minkälaiseen sääntelykehitykseen kyberriskit ovat johtaneet kaupallisen siviili-ilmailun sääntelyssä?*

Ensimmäisellä tutkimusongelmalla keskitytään tutkimaan miten kyberriskit vaikuttavat tai voivat vaikuttaa tällä hetkellä ja lähitulevaisuudessa kaupallisen siviili-ilmailun kyberturvallisuuteen. Vaikutusten tutkimiseksi tutkielmassa selvitetään mitkä kyberriskit koetaan tällä hetkellä ja lähitulevaisuudessa tärkeäksi kaupallisen siviili-ilmailun kyberturvallisuuden kannalta. Ensimmäisen tutkimusongelman osalta tutkielman ytimessä ovat valitun aineiston esittelemät kyberuhkat ja vaikutuskohteet, joiden avulla selvitetään kaupalliseen siviili-ilmailuun vaikuttavia kyberriskejä. Tutkielmassa keskitytään analysoimaan aineistossa eniten esiintyviä kyberuhkia ja vaikutuskohteita sekä vertaamaan niitä kyberriskien teoriaan. Vertaamalla aineiston uh-

kia ja vaikutuskohteita kyberriskin teoriaan tunnistetaan kaupalliseen siviili-ilmailuun tällä hetkellä vaikuttavat kyberriskit. Uhkien ja vaikutuskohteiden analyysillä tunnistetaan kyberriskien vaikutuksia kaupalliselle siviili-ilmailulle.

Kyberriskien maantieteellisten rajojen ylittävän luonteen vuoksi tutkielmassa on kartoitettu kaikkia niitä globaalisti merkittäviä kyberriskejä, joita alalla on tutkittu. Pelkästään kansallisessa käytössä olevista järjestelmistä aiheutuvat kyberriskit on rajattu tutkielmasta pois. Tutkimusongelman tarkoituksena on kartoittaa saatavilla olevista lähteistä alan tärkeäksi kokemat kyberriskit ja niiden vaikutukset, eikä sillä pyritä kartoittamaan alan kaikkia mahdollisia kyberriskejä tai niiden vaikutuksia. Kyberriskien toistaiseksi vakiintumaton määritelmä tieteessä voisi aiheuttaa tutkielmalle laajuuden, joka estäisi oleellisen tiedon esittämisen tutkielman laajuudessa. Rajaus on näin ollen tehty aiheen keskittämiseksi oleelliseen tietoon. Rajauksella pyritään saavuttamaan syvempi tietämys alalle keskeisistä kyberriskeistä.

Toisella tutkimusongelmalla selvitetään, minkälaiseen sääntelykehitykseen kyberriskit ovat johtaneet Euroopan kaupallisen siviili-ilmailun osalta, sekä miten ne tulevat mahdollisesti vaikuttamaan alan tulevan sääntelyn luomiseen. Toisen tutkimusongelman osalta tutkielman ytimessä on Euroopan unionin tekemä sääntely, jota tarkastellaan sääntelykehityksen näkökulmasta. Tutkielma keskittyy selvittämään kyberriskin vaikutuksia sääntelykehitykselle tuomalla esiin Euroopan unionin kyberriskiin keskittyvät direktiivit ja asetukset. Direktiivien ja asetusten sisältöä analysoidaan riskienhallinnan ja hyvän sääntelyn näkökulmista, joiden avulla tuodaan esiin kriittisiä huomioita sääntelyn sisällöstä ja implementoinnista.

Järjestöjen vaikutus kaupallisen siviili-ilmailun sääntelyyn on ollut huomattava jo vuonna 1944 tehdyn Kansainvälisen siviili-ilmailusopimuksen (11/1949) ajoista lähtien. Sopimuksen keskeisenä osapuolena toimi Kansainvälinen siviili-ilmailujärjestö ICAO. Järjestökeskeisyyden vuoksi myös järjestöjen sääntelyyn liittyviä toimia kartoitetaan tutkielmassa. Järjestöjen sääntelytoimien ja Euroopan unionin aloitteiden perusteella pyritään selvittämään myös tulevaisuuden suunta sääntelylle ja sääntelyn edistämistoiminnalle sekä tutkimaan kyberriskien vaikutusta aloitteisiin Euroopassa. Sääntelykehityksen tutkiminen on rajattu koskemaan Euroopan aluetta ja Euroopan sääntelyn omaksumia valtioita, sillä Euroopan ulkopuolinen kansallinen siviili-ilmailun sääntely sisältää monia eroavaisuuksia. Laajempi sääntelyn tarkastelu tekisi tutkielmasta yleisluontoisemman, eikä mahdollistaisi sääntelyyn syventymistä.

Tutkielma käsittelee kyberriskin ilmiötä kaupallisen siviili-ilmailun näkökulmasta, minkä vuoksi siviili-ilmailulla viitataan tutkielmassa kaupallisen siviili-ilmailun kategorian sisältämään ilmailutoimintaan. Kaupallinen siviili-ilmailu kattaa kaiken ilmailutoiminnan, jossa kuljetetaan henkilöitä tai rahtia paikasta toiseen maksua vastaan (IAOPA 2018). Tutkielmasta on rajattu pois yleisilmailun, lentotyön ja valtion harjoittaman ilmailutoiminnan kategoriat, sillä systemaattiseen kirjallisuuskatsaukseen valittu aineisto keskittyy kaupalliseen siviili-ilmailuun. Yleisilmailun, lentotyön, valtion harjoittaman ilmailutoiminnan ja kaupallisen ilmailun sääntelyn eroavaisuuksien osoittaminen ja analysointi heikentäisi tutkielman syvyyttä, minkä vuoksi valittu näkökulma haluttiin säilyttää myös sääntelyn osalta. Näkökulma valittiin myös tutkielman kokonaisuuden eheyden säilyttämiseksi.

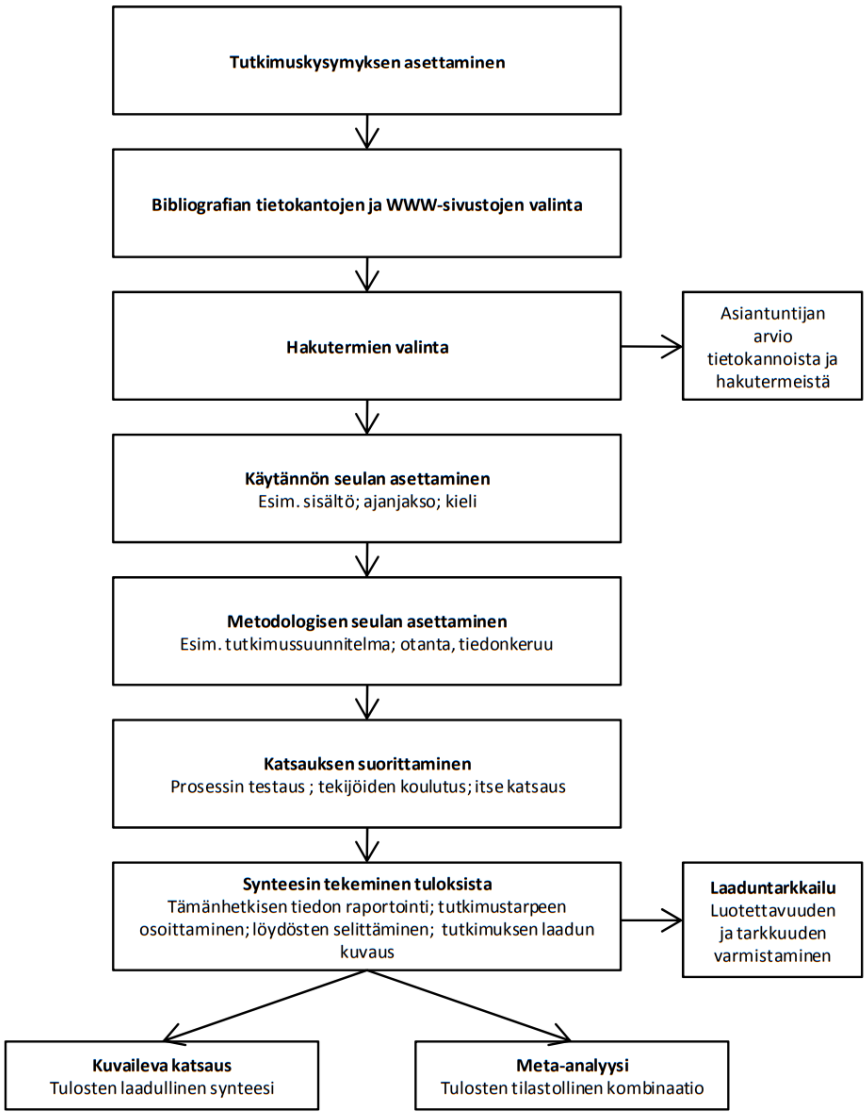
Tutkielma käsittelee kyberriskin vaikutuksia ja sääntelykehitystä kaupallisen siviili-ilmailun toimijoiden näkökulmasta. Kyberriskin vaikutusten osalta toimijoiden näkökulman keskiössä ovat lentokoneiden, lentoyhtiöiden, lentokenttien ja lennonvarmistuspalveluiden teknologiset järjestelmät. Näiden lisäksi toimijoiden näkökulma ottaa huomioon henkilökunnan ja matkustajien käyttämät teknologiset laitteet ja järjestelmät. Sääntelyn osalta käsitellään kaupallisen siviili-ilmailun toimijoihin vaikuttavia direktiivejä, asetuksia, standardeja ja suositeltuja käytäntöjä.

Kyberturvallisuutta on käsitelty tutkielmassa osana kyberriskin käsittelyä. Kyberturvallisuudella tarkoitetaan useissa siviili-ilmailuun keskittyvissä lähteissä ja tutkimuksissa haitallisten hyökkäysten estämisenä ja uhkien torjumisena, jotka ovat kyberriskin hallintamuotoja. Sääntelyssä kyberturvallisuudella tarkoitetaan yleisesti kyberuhkien estämistä ja torjumista. Tämän vuoksi kyberturvallisuuden huomioimista sääntelyssä käsitellään tutkielmassa kyberriskien vaikutuksina sääntelykehitykselle.

1.3 Tutkimusmenetelmät ja aineisto

Tutkielma on toteutettu kirjallisuuskatsauksena aiheen tutkimuksiin. Pääasiallisena tutkimusmenetelmänä toimii systemaattinen kirjallisuuskatsaus, jota täydennetään narratiivisen kirjal-

lisuuskatsauksen menetelmällä sääntelyn tutkimisen osalta. Systemaattisella kirjallisuuskatsauksella seulotaan tulosten kannalta tärkeitä tutkimuksia ja luodaan niiden avulla tiivistelmä aiempien tutkimusten aihepiirille olennaisesta sisällöstä (Salminen 2011, 9).



Kuvio 1 Salmisen malli systemaattisen kirjallisuuskatsauksen vaiheista (2011, 10–11)

Systemaattisella kirjallisuuskatsauksella voidaan esittää tutkimusten tuloksia tiiviissä muodossa ja arvioida tätä kautta tulosten johdonmukaisuutta. Sillä voidaan myös testata hypoteeseja, mutta tässä tutkielmassa hypoteeseja ei ole asetettu, eikä niitä näin ollen testata. Systemaattiselle kirjallisuuskatsaukselle on olennaista referoida tutkimuksia objektiivisesti ja arvioida valittujen tutkimusten laatua. Tämän lisäksi menetelmälle ominaista on vähentää tutkimusten valintaan sisältyvää epäselvyyttä. (Salminen 2011, 9) Tähän pyrittiin käyttämällä soveltaen Salmisen (2011, 10–11) mallia, joka on luotu Finkin (2005) mallia mukaillen.

Kuvion 1 mukaisesti ensin asetettiin tutkimuskysymys, jonka pohjalta materiaalia haettiin. Tutkielmassa systemaattisella kirjallisuuskatsauksella käsitellään kyberriskin vaikutuksia siviili-ilmailuun, sillä kyberriskien Eurooppalaisen sääntelyn vaikutuksista siviili-ilmailuun löytyi vain yksi relevantti hakuosuma.

Näin ollen tutkimuskysymys muotoiltiin systemaattiselle kirjallisuuskatsaukselle seuraavasti:

> *”Mitä kyberriskejä siviili-ilmailussa tunnistetaan ja miten ne vaikuttavat nyt tai voivat tulevaisuudessa vaikuttaa siviili-ilmailuun?”*

Tämän jälkeen valittiin tutkimuksessa käytettävät tietokannat ja verkkosivut. Valinta kohdistui tiedon hajonneisuuden vuoksi mahdollisimman kattavaan tietokantaan, Google Scholariin. Seuraavaksi määriteltiin hakutermit, joiden valintaan vaikutti tutkimuskysymyksen vaikutuskeskeisyys. Tämän vuoksi pelkkiä uhkia kartoittavat tutkimukset ilman mainittuja uhkien vaikutuksia haluttiin jättää sivuun. Keskiöön haluttiin nostaa uhkien ja riskien lisäksi niiden mahdollisia vaikutuksia kyberriskeistä. Aineiston niukkuus aiheesta oli havaittavissa, minkä vuoksi hakutermeiksi valittiin harkinnan ja useiden yhdistelmien testaamisen jälkeen pelkistetysti *”cyber risk”* ja *”aviation”.* Näistä muodostettiin Google Scholariin hakulauseke, jossa molemmat hakusanat sisältyivät otsikkoon. Haulla saatiin kaksi tulosta. Tulosten niukkuuden vuoksi päätettiin lisätä hakutermi *”cybersecurity”* ja muodostaa hakulausekkeet, jossa hakutermit *”cybersecurity”* ja *”aviation”* sisältyvät haettavien tutkimusten otsikkoon, jakaen hakutermi *”cybersecurity”* kahteen osioon kaikkien tulosten löytämiseksi. Näillä hauilla saatiin 31 tulosta.

Google Scholariin syötetyt hakulausekkeet olivat näin ollen:
”intitle:aviation intitle:"cyber security" intext:risk” sekä
”intitle:aviation intitle:cyber intitle:security”.

Tämän jälkeen asetettiin käytännön seulat, jotka voivat Salmisen (2011, 10) mukaan koskea muun muassa sisältöä, ajanjaksoa ja kieltä. Kielen osalta seulaksi asetettiin englanninkielisyys. Sisällön osalta seulaksi asetettiin tutkielman osalta se, että sen tuli käsitellä siviili-ilmailua sekä kyberriskiä tai kyberturvallisuutta. Ajanjaksoksi valittiin 2000-luvun jälkeiset tutkimukset. Käytännön seulan vaatimusten jälkeen tuloksista jäi jäljelle 16, jonka jälkeen asetettiin metodologinen seula.

Metodologisen seulan tarkoitus on arvioida tulosten tieteellistä laatua. Näin pyritään saavuttamaan mahdollisimman laadukas materiaali. (Salminen 2011, 10) Metodologisen seulan kriteerinä toimivat julkaisun julkaisija, saatavuus tietokannasta sekä tutkimuksen vastaavuus asetettuun tutkimuskysymykseen systemaattista kirjallisuuskatsausta varten. Julkaisijana tulee olla yliopisto tai journaali. Tutkimus ei saa olla yrityksen tai oppilaan tekemä, eikä se saa olla rajattu Euroopan ulkopuoliseen kansalliseen siviili-ilmailuun.

Tutkimuksen tulee olla saatavissa Google Scholarin kautta ja kokonaisuudessaan tutkielma tulee olla saatavissa verkossa. Tutkimuksen tulee lisäksi keskittyä pääosaltaan siviili-ilmailuun ja kyberriskiin tai kyberturvallisuuteen, eikä se näin ollen saa keskittyä pääasiallisesti muihin aiheisiin, kuten Yhdysvaltojen ilmailulakiin. Poissulkemiskriteerit asetettiin tutkimusten yhtenäistämiseksi ja asetettuun tutkimuskysymykseen vastaamiseksi.

Taulukko 1 Sisäänottokriteerit ja poissulkemiskriteerit

Sisäänottokriteerit	Poissulkemiskriteerit
Englanninkielisyys	Ennen vuotta 2000 julkaistu
Käsittelee siviili-ilmailua sekä kyberriskiä tai kyberturvallisuutta	Muu kuin journaali tai yliopiston julkaisema julkaisu
Saatavilla Google Scholar-hakupalvelun kautta	Rajaus vain Euroopan ulkopuoliseen kansalliseen siviili-ilmailuun
Saatavilla kokonaisuudessaan verkossa	Oppilaan tai yrityksen tekemä
Keskittyneisyys siviili-ilmailuun	Muu pääasiallinen keskittyneisyys kuin kyberriski tai kyberturvallisuus

Asetettujen kriteerien jälkeen hakutuloksista käytiin läpi sisältö ja karsittiin kriteerien mukaan poissuljettavat tutkimukset. Hakutuloksista jäi jäljelle kolme tulosta. Tutkimusten lukemisen jälkeen aineistoon päätettiin valita poikkeuksena tutkimus ”On Perception and Reality in Wireless Air Traffic Communications Security” (Strohmeier, Schäfer, Pinheiro, Lenders & Martinovic 2017), joka havaittiin Standerin & Ophoffin (2016) tutkimuksen ”Cyber security in civil aviation” lähteistä. Julkaisun ja tekijöiden luotettavuus tarkastettiin ennen julkaisun hyväksymistä kirjallisuuskatsaukseen, minkä lisäksi tarkistettiin, ettei julkaisua käytetä pääasiallisena

lähteenä muissa valituissa tutkimuksissa. Tämän jälkeen sisäänotto- ja poissulkukriteereitä sovellettiin tutkimukseen ja todettiin tutkimuksen täyttävän asetetut vaatimukset. Poikkeusvalinta tehtiin sisällön laaja-alaisuuden ja kysymykseen vastaavuuden vuoksi. Tutkimus on julkaistu kansainvälisen tekniikan alan järjestö IEEE:n journaalissa sekä Oxfordin yliopiston sivuilla (University of Oxford 2017). Valitut tutkimukset olivat näin ollen seuraavat:

Taulukko 2 Valitut tutkimukset perustietoineen

Numero	**Otsikko**	**Tekijät ja julkaisuvuosi**	**Julkaisun alkuperä**	**Julkaisun keskeiset havainnot**
T1	**Aviation and Cybersecurity: Opportunities for Applied Research**	Jon Haass, Radhakrishna Sampigethaya, Vincent Capezzuto 2016	Embry Riddle Aeronautical University, Aviation Security Commons	Useat järjestelmät ovat alttiita kyberuhkille. Uhkat kyberturvallisuudelle ovat merkittävä haaste ilmailulle.
T2	**Cyber security in civil aviation**	Adrie Stander, Jacques Ophoff. 2016	Imam Journal of Applied Sciences. Vol. 1, iss. 1. pp. 23-26	Kyberhaavoittuvuuksia löytyy useista järjestelmistä. Kyberhyökkäyksen todennäköisyys on matala.
T3	**Aviation Cybersecurity: An Overview**	Gary C. Kessler, J. Philip Craiger. 2018	National Training Aircraft Symposium, Embry Riddle Aeronautical University	Kyberuhkia voidaan vähentää, mutta niitä ei voida poistaa. Kyberhyökkäykset uhkaavat ilmailualan olemassaoloa, ellei niihin reagoida.
T4	**On Perception and Reality in Wireless Air Traffic Communications Security**	Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders & Ivan Martinovic 2017	Journal of IEEE Transactions on Intelligent Transportation Systems, Vol. 18, pp. 1338–1357	Ilmailualan turvallisuus on jäljessä langattomien järjestelmien osalta.

Tutkielmassa pyritään kartoittamaan kyberriskiä siviili-ilmailussa arvioivat tutkimukset ja tiivistämään niistä oleellinen tieto tutkielmaan. Tutkielmalla pyritään tiivistämään aiheelle olennainen materiaali ja vetämään sen avulla johtopäätöksiä aiheelle merkittävällä ja tutkimusongelmiin kattavasti vastaavalla tavalla. Salmisen (2011, 9) mukaan myös laaja työ voi olla lähteiden valinnoiltaan yksipuolinen, eikä laaja-alaisuus näin ollen toimi arvona sinänsä. Tämän vuoksi lähteiden valinnassa keskityttiin erityisesti siihen, että sisältö vastaa tutkimuskysymykseen. Petticrewn (2001, 99) mukaan systemaattisen kirjallisuuskatsauksen tehtävänä on vastata määritettyyn kysymykseen, vähentää ennakkoluuloja tutkimusten valinnasta ja sisällyttämisestä, arvioida sisällytettyjen tutkimusten laatua sekä tehdä niistä objektiivinen yhteenveto. Tämän seurauksena systemaattinen kirjallisuuskatsaus voi olla aineistoltaan muita kirjallisuuskatsauksia pienempi, sillä aineiston valintaan sisällytetään tarkemmat kriteerit (Petticrew 2001, 99). Systemaattista kirjallisuuskatsausta pidetään Tuomen & Sarajärven (2018, 138) mukaan tehokkaana välineenä syventää tietoja asioista, joista on jo valmista tutkittua tietoa ja tuloksia.

Kvalitatiivisessa tutkimuksessa analyysiä tehdään pitkin tutkimuksen matkaa, jonka vuoksi aineistoa analysoitiin jo läpilukuvaiheessa synteesin luomiseksi (Hirsjärvi, Remes & Sajavaara 2009, 223). Analysoinnin menetelmänä käytettiin aineistolähtöistä analyysiä, jonka avulla valittiin aineistosta analyysiyksiköt tarkoituksen ja tehtävänasettelun mukaisesti. Analyysiyksiköt eivät olleet etukäteen sovittuja tai harkittuja, mikä on aineistolähteisen analyysin perusta. (Tuomi & Sarajärvi 2018, 108).

Analyysiyksiöiden avulla aineistosta tehtiin synteesi taulukkoon 4. Synteesin avulla kerättyä aineistoa analysoitiin sisällönanalyysillä. Analyysi toteutettiin ymmärtämiseen pyrkivällä lähestymistavalla, jossa käytettiin laadullista analyysiä ja pyrittiin tekemään päätelmiä aineistosta. Yhteenvetolukuun tehtiin analyysistä tulkintoja, joiden tarkoitus on pohtia analyysin tuloksia ja tehdä tuloksista johtopäätöksiä. (Hirsjärvi ym. 2009, 224, 229)

Sääntelyn osalta tutkimusmenetelmäksi valittiin narratiivinen kirjallisuuskatsaus. Narratiivisen kirjallisuuskatsauksen avulla voidaan antaa laaja kuva sekä käsitellä kehityskulkua valitusta aiheesta. Narratiivinen kirjallisuuskatsaus auttaa ajantasaistamaan tutkimustietoa (Salminen 2011, 7), mikä on tutkielman aiheen ajankohtaisuuden ja käsittelemättömyyden vuoksi tärkeää. Yhtenäistä määritelmää kyberriskistä ei vielä ole syntynyt, eivätkä siviili-ilmailun toimijat

käsittele kyberriskiä yhtenäisen määritelmän pohjalta. Tämän vuoksi on tärkeää myös ajantasaistaa tutkimustietoa ja luoda yhtenäinen tiivistelmä aiheen sääntelystä ja muusta saatavasta materiaalista.

Tutkimukset eivät ole keskittyneet kyberriskin vaikutuksiin Euroopan sääntelyssä, minkä vuoksi päätettiin tutkia Euroopan unionin asetuksia ja direktiivejä sekä siviili-ilmailun virallisten järjestöjen julkaisuja. Sääntelyä etsittiin hakutermeillä *”civil-aviation”, ”cyber risk” ja ”cyber security”* käyttäen hakemistona Euroopan unionin lakikokoelma EUR-lexiä. Hakua vastaavista asetuksista ja direktiiveistä tarkistettiin niitä edeltäneet asetukset ja direktiivit, joita asetus on muokannut tai jotka asetus on korvannut. Tämän jälkeen relevanteiksi osoittautuneet asetukset ja direktiivit luettiin läpi ja niistä koottiin tutkielman kannalta merkittävä tieto.

Järjestöjen osalta katsaukseen sisällytettiin vain sellaisten järjestöjen julkaisut, joilla on aktiivinen rooli yhteistyötekijänä Euroopan unionin kanssa tai aktiivinen rooli lainsäädännön edistämisessä Euroopan unionissa. Järjestöiksi valikoitui tätä kautta Euroopan lentoturvallisuusvirasto, Kansainvälinen siviili-ilmailuvirasto, Euroopan siviili-ilmailun konferenssi sekä Kansainvälinen lentoliikennöintiyhtiöiden järjestö International Airline Traffic Association. Tämän lisäksi poikkeuksena otettiin järjestöihin Euroopan alueellisten lentoyhtiöiden liitto, jonka kautta voidaan tarkastella lainsäädännön käytännön vaikutuksia Euroopan siviili-ilmailuun. Järjestöjen sivuilta etsittiin termeillä *”cyber risk”* ja *”cyber security”*. Hakua vastanneet tulokset luettiin läpi ja ne seulottiin sisällön perusteella jättäen tulokseksi yhden julkaisun. Julkaisusta sisällytettiin tutkielmaan olennaiset osat Eurooppalaisen sääntelyn vaikutusten osalta. Aineiston perusteella pyritään antamaan laajempaa kuvaa ilmiöstä sekä sääntelyn kehityskulusta, jotka ovat Salmisen (2011, 7) mukaan narratiivisen kirjallisuuskatsauksen tehtäviä.

Myös narratiivisen kirjallisuuskatsauksen avulla kerätystä materiaalista tehtiin analyysiä jo lukuvaiheessa synteesin luomiseksi käyttämällä aineistolähtöistä analyysiä. Aineistoa yhdisteltiin erottaen tutkimuksen kannalta oleellinen tieto. Synteesin kautta saatua tietoa analysoitiin edelleen sisällönanalyysin menetelmällä. Analyysin sisällöstä tehtiin myös tulkintoja yhteenvetolukuun, joilla pyrittiin pohtimaan ja selkeyttämään esiin nousevia merkityksiä (Hirsjärvi ym. 2009, 229).

Kahden tulokulman yhteismenetelmä auttaa keräämään julkisena olevan tiedon monipuolisista lähteistä, minkä avulla saadaan pelkkää systemaattista kirjallisuuskatsausta laajempi materiaali ilmiöstä. Laajempi materiaalipohja varmistaa johtopäätösten ja analyysin syvyyttä. Materiaalia laajennettiin näin ollen siviili-ilmailun järjestöjen ja liittojen verkkojulkaisuilla ja Euroopan unionin virallisilla internet-lähteillä. Sääntelyn implementoinnin esittelyyn valittiin myös Trafin ja Valtioneuvoston verkkomateriaalia.

Tutkielman tarkoituksena on tutkia myös siviili-ilmailun toimijoiden ja sen sääntelijöiden tietoisuuden tilaa kyberriskeistä, joita tutkitaan kyberriskien vaikutusten kautta. Tämä noudattaa kirjallisuuskatsauksen tyyppiä, jonka tarkoituksena on tietyn aiheen tietoisuuden tilaa kartoittava kirjallisuuskatsaus. Tämän tyypin kirjallisuuskatsauksella pyritään tarjoamaan hyödyllisiä yhteenvetoja aiheesta. (Baumeister & Leary 1997, 2)

Kirjallisuuskatsauksen valinnan perusteena haastattelujen sijaan toimi aiheen luonne, joka estäisi haastateltavia kertomasta muita kuin julkisia tietoja aiheen osalta. On ymmärrettävää, ettei verrattain uuden riskin osalta, johon ei organisaation mielestä välttämättä ole ehditty varautumaan tarpeeksi kattavissa määrin, haluta paljastaa lisätietoja kenellekään ulkopuoliselle. Organisaatioiden riskienhallinnan näkökulmasta vaikutus on vielä ilmeisempi, sillä lisätiedon antaminen aiheesta voisi asettaa organisaation vaaraan.

1.4 Keskeiset käsitteet

Siviili-ilmailu – Siviili-ilmailulla tarkoitetaan kaikkea ilmailutoimintaa, mikä ei ole valtion harjoittamaa. Siviili-ilmailu voidaan jakaa yleisen ilmailun, lentotyön ja kaupallisen ilmailutoiminnan kategorioihin. Yleiseen ilmailun kategoria sisältää muun muassa yhtiöiden sisäisen lentotoiminnan, yksityisen lentomatkustamisen, lentoturismin ja harrastuslentämisen. Lentotyön kategoriaan kuuluvat muun muassa ilmakartoitus, maatalouden lentotoiminta, lentomainostus, lentäjien koulutuslennot ja sairaalalennot. Kaupallinen ilmailutoiminta kattaa kaiken reittilentämisen, tilauslentämisen ja rahtilentämisen. Kaupallinen siviili-ilmailu kattaa kaiken ilmailutoiminnan, missä kuljetetaan henkilöitä tai rahtia paikasta toiseen maksua vastaan. (IAOPA 2018)

Kyberriski – Kyberriski kattaa kaikki ne riskit, jotka johtavat taloudelliseen menetykseen, toiminnan keskeytymiseen tai vahingoittavat organisaation mainetta ja aiheutuvat informaatioteknologisesta virheestä. Informaatioteknologiset virheet käsittävät kaikki heikosta järjestelmästä johtuvat operationaaliset virheet, tahalliset ja auktorisoimattomat tietomurrot sekä vahingolliset ja tahattomat tietomurrot. (Institute of Risk Management 2014, 8)

Kyberuhka – Järjestelmän turvallisuuden, tietojen luottamuksellisuuden, tiedon saatavuuden tai tietojen eheyden vaarantava mahdollisuus, joka voi vaikuttaa myös toimintoihin, jotka varmistavat tietojen aitouden ja kiistämättömyyden. (Banta 2012, 9)

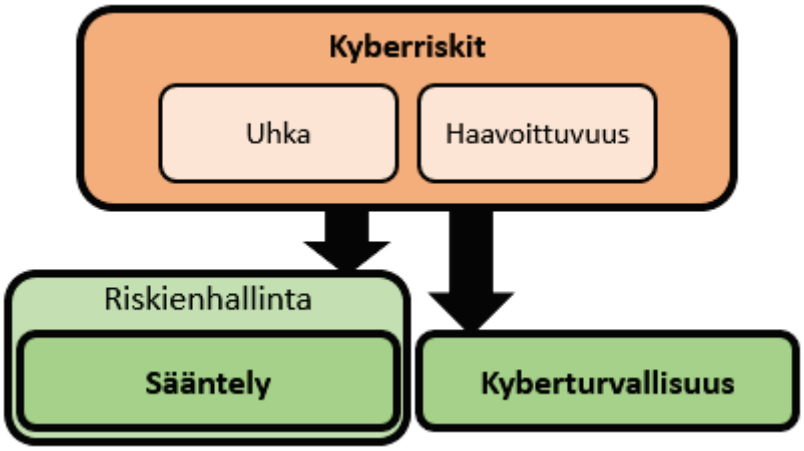
Haavoittuvuus – Kyberhaavoittuvuus on virhe tai heikkous järjestelmäturvallisuuden suunnittelussa tai implementoinnissa. Kyberhaavoittuvuudella voidaan tarkoittaa myös järjestelmään kohdistettujen turvatoimien virhettä tai heikkoutta suunnittelu- tai implementointivaiheessa, joita voidaan hyväksikäyttää tahallisesti tai tahattomasti. (Banta 2012, 10)

Kyberturvallisuus – Kyberturvallisuudella tarkoitetaan digitaalisen maailman tilaa, jossa vallitsee käytännön toimenpitein saavutettu kyky ennakoivasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia. Kyberturvallisuuteen huomioidaan myös ymmärryksen myötä tuotettu luottamuksen tunne. (Limnéll, Majewski & Salminen 2014, 39)

Sääntely – Sääntely on julkisen tahon jatkuvaa ja keskitettyä valvontaa, joka keskittyy yhteisön arvostamiin aktiviteetteihin (Selznick 1985, 363). Sääntelyn merkitys voidaan nähdä kokoelmana käskyjä tai toimintaohjeita, tarkoituksellisena valtion vaikutusvaltana sekä talouden ja sosiaalisen vaikutusvallan kaikkina muotoina (Baldwin, Cave & Lodge 2011, 2–3).

1.5 Teoreettinen viitekehys

Tutkielmassa pyritään muodostamaan kokonaiskuva yhdistelemällä aiemmin yhteen sovittamattomia teorioita ja empiirisiä havaintoja. Tämän vuoksi tutkimus on syntetisoiva teoreettinen tutkimus (Uusitalo 2001, 61). Tutkielmassa yhdistyvät kyberriskit, sääntely ja kyberturvallisuus, joilla pyritään muodostamaan kokonaiskuva Eurooppalaisen siviili-ilmailun kyberturvallisuudesta kyberriskien näkökulmasta.



Kuvio 2 Tutkielman teoreettinen viitekehys

Uusitalon (2001, 42) mukaan viitekehyksellä on tarkoitus tuoda esille se, mihin aikaisempiin tieteellisiin tutkimuksiin tai keskusteluihin tutkimus liittyy sekä se, millaisen käsitteistön valossa kohdeilmiötä tarkastellaan. Kuviossa 2 kuvataan tutkielman teoreettisen viitekehyksen teoriat, joista taustateoriana on kyberriskit ja tulkintateorioina riskienhallinta, sääntely ja kyberturvallisuus. Kyberriskit toimivat näkökulmana, mistä ilmiöiden tarkastelu tapahtuu. Uhkat ja haavoittuvuudet toimivat kyberriskin osina, minkä vuoksi ne on kuvattu kuviossa osaksi kyberriskejä.

Tutkielmassa tutkitaan kyberriskien vaikutusta Euroopan siviili-ilmailun sääntelylle ja kyberturvallisuudelle, minkä vuoksi kyberriskistä on johdettu kaksi nuolta. Toinen nuolista etenee suoraan kyberturvallisuuteen, selkeyttäen tutkimusasetelmaa sekä tausta- ja tulkintateorian yhteyttä. Kyberriskien vaikutusta sääntelyyn havainnoidaan nuolella riskienhallintaan ja sääntelyyn. Sääntelyä tutkitaan tutkielmassa osana riskienhallintaa, minkä vuoksi riskienhallinta on kuvattu kuviossa sääntelyn ympärille. Sääntelystä tehdään johtopäätöksiä myös hyvän sääntelyn teoriaan verraten. Hyvän sääntelyn teoriaa ei kuitenkaan käytetä tutkimusongelmiin vastattaessa, minkä vuoksi sitä ei ole sisällytetty teoreettiseen viitekehykseen omana osionaan.

1.6 Aikaisemmat tutkimukset ja rakenne

Kyberriskien vaikutukset siviili-ilmailuun, ja erityisesti sen kyberturvallisuuteen, on aiheena uusi, minkä vuoksi aiheesta ei ole tehty merkittävää määrää tutkimusta. Kokoavaa tutkimusta

aihepiiristä ei löydetty systemaattiseen kirjallisuuskatsaukseen valittujen teosten ulkopuolelta. Maailmanlaajuisesti tutkimusta kyberriskeistä siviili-ilmailussa on tehty järjestelmien analyysien kautta, mutta riskejä kokoavaa kirjallisuutta on hyvin vähän.

Tutkielmaan sisällytetyn aineiston lisäksi järjestelmäanalyysejä on tehty muun muassa lentokoneen viihdejärjestelmästä (FAA 2008) ja ADS-B-järjestelmästä (Kacem, Wijesekera, Costa, Monteiro & Barreto 2015; Leonardi, Piracci & Galati 2012). Analyysit keskittyvät kuitenkin yhden järjestelmän toimintaan ja analysoivat järjestelmien vikatiloja, eivätkä näin ollen keskity yksinomaan kyberriskeihin tai kyberturvallisuuteen.

Pääasiallisena tehtävänään siviili-ilmailun kyberturvallisuuteen vaikuttavia riskejä, uhkia ja haavoittuvuuksia keräävät ja käsittelevät tutkimukset on sisällytetty systemaattisen kirjallisuuskatsauksen aineistoon. Aiheen tutkimattomuuden osoittaa myös Google Scholar-hakukoneella tehty haku, jossa on sisällytetty hakusanoihin tutkimukset, joiden otsikossa esiintyy sanat aviation, cyber ja risk. Hakutermillä *"intitle:aviation intitle:cyber intitle:risk"* saadaan vain kaksi tulosta. Kokoavista tutkimuksista pois jätettiin De Cerchion & Rileyn (2011) tutkimus siviili-ilmailun kyberturvallisuudesta, sillä se keskittyi pääosin Yhdysvaltojen sääntelyn edistämiseen. Young, Lopez Jr., Rice, Ramsey & McTasney (2016) ovat tutkineet kriittisten infrastruktuurien kyberriskejä, sekä niiden vakuuttamista. Tutkimus keskittyy kaikkiin kriittisiin infrastruktuureihin ja vakuuttamisen näkökulmaan.

Kyberriskien vaikutuksista siviili-ilmailun sääntelyyn Euroopassa ei ole myöskään tehty kattavaa tutkimusta. Fahey (2014) on tutkinut Euroopan unionin kyberrikollisuuden ja kyberturvallisuuden sääntelyn laatimista, mutta tutkimus ei mainitse ilmailua tai keskity ilmailuun. Urban (2017) puolestaan on tutkinut kyberriskin vaikutuksia sääntelyyn Yhdysvalloissa, mutta tutkimus keskittyy pääasiallisesti Yhdysvaltojen kansalliseen sääntelyyn, käytäntöihin ja standardeihin. Tutkimuksen puutteen vuoksi tutkielmassa keskityttiin sääntelyn osalta kartoittamaan olemassa olevaa sääntelyä ja tarkastelemaan mahdollista tulevaa sääntelyä, joka koskettaa siviili-ilmailua ja kyberturvallisuutta.

Tutkielman rakenne noudattaa vakuutustieteen ohjetta sisältäen kuusi päälukua. Pääluvuista ensimmäinen on johdanto, kaksi seuraavaa ovat teorialukuja, niistä seuraavat kaksi ovat empirialukuja ja viimeisenä lukuna on yhteenveto. Johdantoluvussa käydään ensin läpi aiheen

taustaa, jonka jälkeen esitellään tutkielman tavoitteet, tutkimusongelmat, rajaukset, aineistonvalinta, keskeiset käsitteet ja aikaisemmat tutkimukset. Johdannon tarkoituksena on antaa lukijalle kuva aiheesta sekä siitä, mitä tutkielmassa tutkitaan ja mitä tieteellisiä valintoja tutkielmaan on sisällytetty.

Luvussa kaksi käsitellään kyberriskeihin liittyvää teoriaa ja esitellään kyberturvallisuuden näkökulma ja merkitys. Lisäksi luvussa syvennytään kyberriskien luokitteluun, vaikutuksiin ja hallintaan. Kyberriskit toimivat tutkielman taustateoriana, minkä vuoksi luku esitellään ensimmäisenä kahdesta teorialuvusta. Kyberturvallisuus on valittu tutkielman tulkintateoriaksi, minkä vuoksi sen merkitystä avataan erikseen ensimmäisessä teorialuvussa.

Kolmannessa luvussa käsitellään sääntelyä osana riskienhallintaa sekä esitellään sääntelyn tarkoitusta ja luonnetta. Luvussa tuodaan myös esille näkemyksiä hyvästä sääntelystä, mikä antaa pohjaa analyysin ja johtopäätöksen tekemiselle tutkielmassa käsiteltävästä sääntelystä. Luvussa syvennytään ilmailualan sääntelyyn ja sääntelijöihin, jotta lukijalle voidaan esitellä siviili-ilmailua koskeva Euroopan unionin sääntelyprosessi, sen vaiheet ja sen vaikuttajat. Prosessin, vaiheiden ja vaikuttajien esittely toimii myös pohjana analyysin ja johtopäätösten tekemiselle.

Neljännessä luvussa tehdään systemaattisen kirjallisuuskatsauksen aineistosta synteesi ja analyysi. Synteesin välineenä toimii taulukko, jonka avulla tutkimusten tunnistamat kyberriskien vaikutuskohteet siviili-ilmailussa asetetaan esiintymien perusteella taulukkoon. Taulukon avulla voidaan löytää yhteneväisyyksiä tutkimuksista. Yhteneviä vaikutuskohteita analysoidaan tarkemmin tutkimusten pohjalta ja analyysin pohjalta tehdään havaintoja. Luvussa käsitellään myös toimijoiden näkökulmaa kyberriskien vaikutuksesta kyberturvallisuuteen. Käsittely tapahtuu luvussa 1.3 esitellyn materiaalin pohjalta. Aineistosta nostetaan esiin tutkielmalle merkittävä sisältö ja analysoidaan sitä. Analyysin lisäksi sisällöstä tehdään havaintoja kyberriskien vaikutuksesta kyberturvallisuuteen toimialan toimijoiden näkökulmasta. Kahdella eri aineistolla pyritään antamaan kattavampi kuva tutkittavasta ilmiöstä.

Luvussa viisi käsitellään kyberriskien vaikutusta Euroopan siviili-ilmailun sääntelyyn esittelemällä Euroopan sääntelyn lisäksi myös luvussa 1.3 esitellyt aineistot. Luvussa nostetaan esiin aineistosta löytyneet merkittävät sääntelyn kohdat ja järjestöjen julkaisujen kohdat, minkä jälkeen niitä analysoidaan ja niistä tehdään havaintoja. Laajennetulla aineistolla ja analyysin

avulla pyritään luomaan kattava yhteiskuva kyberriskien vaikutuksista sääntelyyn tällä hetkellä.

Kuudennessa luvussa vastataan tutkimusongelmiin ja esitellään tutkielman johtopäätökset tutkielman aineiston, tehdyn synteesin ja suoritetun analyysin avulla. Tämän lisäksi viimeisessä luvussa arvioidaan tutkielman luotettavuutta sekä sen aineiston laatua ja luotettavuutta. Kuudennen luvun lopuksi arvioidaan kyberriskien, kyberturvallisuuden ja sääntelyn tulevaisuuden suuntaa sekä esitellään mahdollisia jatkotutkimuskohteita.

2 KYBERRISKIT

2.1 Kyberriskin olemus

Fyysisen maailman lisäksi ihmisiä ympäröi kybermaailma, joka koostuu digitaalisesta ulottuvuudesta ympärillämme. Kybermaailma käsittää muun muassa koko internetin, erilaiset tietoverkot, tietojärjestelmät, sosiaalisen median ja älypuhelimen ohjelmistot. Nykyaikana termi ”kyber” on osana jokapäiväistä toimintaamme ja hyväksymme passiivisesti kybertoiminnan olevan suurena osana elämäämme. Fyysinen maailma ja kybermaailma ovat nykypäivänä sulautuneet vahvasti yhteen ja fyysinen maailma on tullut riippuvaiseksi kybermaailman toimivuudesta. Innovaatiot kybermaailman osalta ovat parantaneet yritysten tehokkuutta ja yksilöiden elämänlaatua, mutta jatkuva kehitys saattaa fyysistä maailmaa yhä enemmän riippuvaiseksi kybermaailman toimivuudesta. Kybermaailman häiriö vaikuttaa näin ollen fyysisen maailman toimivuuteen aiheuttaen kyberriskejä ja kyberuhkia. (Limnéll ym. 2014, 31–32)

Yritysten, julkisyhteisöjen ja ihmisten toiminta riippuu usein teknologian toiminnasta, mutta teknologia ja siihen liittyvät riskit jäävät helposti näkymättömiksi. Kyberriski ei ole vain teknologinen ongelma, vaan se koskettaa riskinä kaikkia toimialoja ja kaikkea yritystoimintaa. Kyberriski muodostuu teknologian lisäksi ihmisten toiminnasta niin yrityksen sisällä kuin ulkopuolellakin. (Ulsch 2014, xv–xvi) Kyberriski on Hamptonin (2015, 201) mukaan aineetonta tai aineellista, vakuutettavaa tai ei vakuutettavissa olevaa riskiä, joka aiheutuu teknologiasta ja keskittyy laitteistoon sekä järjestelmiin, jotka tukevat yritystoimintaa. Kyberriski pohjautuu

terminä riskin lähteisiin, jotka vaikuttavat yrityksen omistuksessa olevaan informaatioon ja teknologiaan. Kyberriskiä on määritelty usealla eri tavalla eikä yksimielistä vakiintunutta määritelmää ole vielä syntynyt. (Biener, Eling & Wirfs 2015) Useat määritelmät koskettavat vain yhtä tai muutamaa osa-aluetta kyberriskin kuvaamiseen, kuten identiteettivarkautta, arkaluontoisen tiedon paljastumista tai toiminnan keskeytymistä teknologisten järjestelmien häiriön vuoksi. Toisissa määritelmissä kyberriski määritellään toimijan aikomusten mukaan rajaten kyberriskit tahalliseen haitalliseen toimintaan. (Eling & Schnell 2016, 475)

Kyberriski sisältää kuitenkin useita osa-alueita, joita painottavat Cebula ja Young (2010) määrittelevät kyberriskin laajemmin informaatiota ja teknologiaa koskevina operationaalisina riskeinä, jotka vaikuttavat tiedon tai järjestelmän luottamuksellisuuteen, saatavuuteen tai eheyteen. Institute of Risk Management (2014, 8) määrittelee kyberriskin kattavan kaikki ne riskit, jotka johtavat taloudelliseen menetykseen, toiminnan keskeytymiseen tai vahingoittavat organisaation mainetta ja aiheutuvat informaatioteknologisesta virheestä. Informaatioteknologiset virheet käsittävät kaikki heikosta järjestelmästä johtuvat operationaaliset virheet, tahalliset ja auktorisoimattomat tietomurrot sekä vahingolliset ja tahattomat tietomurrot. (Institute of Risk Management 2014, 8)

Kyberriskeistä ja siihen läheisesti liittyvästä kybervakuuttamisesta ei ole tehty laajalti tutkimuksia, mutta tutkimusten määrä on kasvanut räjähdysmäisesti vuoden 2010 jälkeen, mikä osoittaa riskin ajankohtaisuuden. Kyberriskitutkimus on keskittynyt pääosin informaatioteknologian puolelle eikä riskiä ole laajalti käsitelty muista, kuten esimerkiksi kauppatieteiden näkökulmasta. (Eling & Schnell 2016, 474–486)

Termi ”kyber” sisältää kaksi elementtiä, jotka ovat tietoverkostot ja virtuaalitodellisuus. Nämä elementit erottavat kyberriskit muista riskeistä, sillä virtuaalitodellisuus korostaa riskin aineettomuutta ja täten riskin vaikutusten määrittelyn vaikeutta. Tietoverkostot taas kuvaavat riskin laajuutta ja lähdettä, sillä tietoverkostot käsittävät internetin lisäksi kaikki muut verkostot, jotka liittävät informaatioteknologiset järjestelmät toisiinsa. Useat perinteiset riskit eivät myöskään korreloi keskenään, kun taas kyberriskeillä on potentiaalisesti hyvin vahva korrelaatio keskenään tehden riskistä hankalamman mallintaa. Mallintamista ja kyberriskien hallitsemista vaikeuttaa myös maantieteellisen sijainnin merkityksen heikentyminen kyberriskien globaalin olemuksen vuoksi. Maantieteellisellä sijainnilla ei ole väliä, mikäli järjestelmät ovat yh-

teyksissä toisiinsa, jolloin riski voi aiheutua toisessa maanosassa ja vaikuttaa sitä kautta kaikkiin yhteyksissä oleviin laitteisiin ja yrityksiin. Saman asetelman vuoksi myös laitteistojen turvallisuuden ylläpito voi osoittautua haasteelliseksi, sillä yhden laitteen vika tai turvallisuusaukko voi mahdollistaa sisäänpääsyn koko tietoverkkoon ja sitä kautta myös muihin laitteisiin. Kyberriskit ovatkin näin ollen luonteeltaan vahvasti keskenään korreloivia ja globaaleja ja voivat aiheuttaa merkittäviä niin pitkän kuin lyhyenkin aikavälin vahinkoja. (Eling & Schnell 2016, 475–477)

Vahinkojen arviointi on kyberriskien kohdalla erityisen haastavaa, sillä hyväksyttyjä tietolähteitä kustannusten virallisesta määrästä ei ole olemassa ja arviointiin liittyy aina suuri epävarmuus. Osa toteutuneista kyberriskeistä, kuten kyberrikollisuus, ei välttämättä aiheuta kohteelle mitään kustannuksia tai kustannuksia ei voida määrittää. Vahinkojen arvioinnin lisäksi kyberriskiä on vaikea mallintaa eikä vakiintunutta mallia kyberriskin mallintamiselle ole kehitetty. Kyberriskin monimuotoisuus ja korreloiva luonne vaikeuttavat mallintamista. (Eling & Schnell 2016, 477–478)

2.2 Kyberriskien luokittelu

Kyberriskejä voidaan luokitella monen eri toiminnon pohjalta, mutta suurin osa näistä luokitteluista jättää merkittävän osan riskeistä käsittelemättä keskittyen kriteereiltään yhteen tarkempaan kategoriaan. Mikään taulukko ei todennäköisesti ole tyhjentävä kyberriskien muuttuessa ja muokkaantuessa jatkuvasti, mutta Cebulan ja Youngin (2010) operationaalisten kyberriskien taulukko (Taulukko 3) kokoaa merkittävät operationaaliset kyberriskit selkeästi jaoteltuun kompaktiin muotoon.

Taulukko 3 jakaa kyberriskit neljään eri kategoriaan, joita ovat ihmisten toiminta, järjestelmähäiriöt ja tekniset viat, epäonnistuneet sisäiset prosessit ja ulkoiset tapahtumat. Neljän pääluokan lisäksi taulukko jakaa jokaisen ongelman alaluokkiin, joiden alle on listattu elementtejä riskiä aiheuttavista pääasiallisista alakategoriaan vaikuttavista operationaalisista toimista. Kyberriskien hallinta on usein keskitetty informaation ja teknologian operationaalisiin riskeihin. Ihmisten toiminta ja kiinteistöön liittyvät riskit nähdään usein tukitoimintoina, jolloin niihin liittyvien riskien nähdään vaikuttavan informaatioon ja teknologiaan välillisesti. Taulukoinnin

ja kyberriskien kokonaisuuden tutkimisen kannalta on tärkeää huomioida, että kyberriskit korreloivat usein keskenään ja voivat aiheuttaa tapahtumasarjan laukaisten useampien riskien toteutumisen yhden riskin toteutuessa. (Cebula & Young 2010)

Taulukko 3 Operationaalisten kyberriskien luokittelu (mukaillen Cebula & Young 2010)

1. Ihmisten toiminta	2. Järjestelmähäiriöt ja teknologiset viat	3. Epäonnistuneet sisäiset prosessit	4. Ulkoiset tapahtumat
1.1 Tahattomuus Vahingot Virheet Laiminlyönnit **1.2 Tahallisuus** Petokset Sabotoinnit Varkaudet Vandalismi **1.3 Toimettomuus** Taidot Tiedot Ohjaus Saatavuus	**2.1 Laitteisto** Kapasiteetti Suorituskyky Huolto Vanhentuneisuus **2.2 Ohjelmisto** Yhteensopivuus Konfiguroinnin hallinta Muutosten kontrollointi Turvallisuus-asetukset Ohjelmointikäytännöt Testaus **2.3 Järjestelmät** Suunnittelu Tekniset vaatimukset Integraatio Monimutkaisuus	**3.1 Prosessien suunnittelu ja toteutus** Prosessin kulku Prosessin dokumentointi Roolit ja vastuut Ilmoitukset ja hälytykset Informaation kulku Ongelmien kasvaminen Palvelutasosopimukset Tehtäviensiirto **3.2 Prosessin kontrollointi** Tilan valvonta Mittarit Jaksottainen arviointi Prosessin omistajuus **3.3 Tukitoiminnot** Henkilöstöhallinta Rahoitus Kehitys- ja koulutustoiminta Hankinta	**4.1 Katastrofit** Sääilmiöt Tulipalot Tulvat Maanjäristykset Levottomuudet Pandemiat **4.2 Lainsäädännölliset ongelmat** Sääntelyn noudattaminen Lainsäädäntö Oikeudenkäynnit **4.3 Liiketoiminnan ongelmat** Tavarantoimittajan häiriö Markkinaolosuhteet Taloudelliset olosuhteet **4.4 Riippuvaisuussuhteet** Sähkö-, vesi- ja tietoliikenneverkot Pelastustoimipalvelut Varavoima Kuljetus

Taulukossa 3 ensimmäisenä kategoriana oleva ihmisten toiminta kuvaa operationaalista riskiä, joka aiheutuu joko ihmisten toiminnasta tai toimimatta jättämisestä. Kategoria on jaettu kol-

meen alaluokkaan; tahattomuuteen, tahallisuuteen ja toimettomuuteen. Tahattomuuden alaluokka sisältää kaikki ne organisaation sisäisten tai ulkopuolisten henkilöiden toimet, jotka aiheutuvat tahattomasti ilman vahingollista aikomusta. Alaluokka on jaettu kolmeen elementtiin, joita ovat vahingot, virheet ja laiminlyönnit. Tahallisuuden alaluokka käsittää kaikki organisaation sisäisten ja ulkoisten henkilöiden toimet, jotka on suunnattu tarkoituksellisesti tuottamaan vahinkoa. Alaluokka on jaettu petoksen, sabotoinnin, varkauden ja vandalismin elementteihin. Toimettomuuden alaluokalla tarkoitetaan organisaation henkilöiden toimimattomuutta, toteuttamatta jättämistä tai tekemättömyyttä, joka aiheuttaa organisaatiolle vahinkoa. Toimettomuuden aiheuttavia elementtejä voivat olla taitojen puute, tiedon puute, ohjauksen puute tai resurssien saatavuuden puute. (Cebula & Young 2010)

Toinen kategoria taulukossa 3 käsittää järjestelmävirheet ja teknologiset viat, sisältäen virheellisen, epänormaalin ja odottamattoman järjestelmän toiminnan, joka voi aiheuttaa organisaatiolle vahinkoa. Kategoria on jaettu kolmeen alaluokkaan, joita ovat laitteisto, ohjelmisto ja järjestelmät. Laitteiston toiminnan kannalta riskielementtejä ovat kapasiteetin riittämättömyys, puutteellinen suorituskyky, huollon epäonnistuminen ja laitteiston vanhentuneisuus. Ohjelmiston alaluokka käsittelee kaikista ohjelmistoista, kuten ohjelmista, applikaatioista ja toimintajärjestelmistä johtuvaa riskiä. Näiden toiminnan kannalta keskeisiä riskielementtejä ovat yhteensopivuus, konfiguroinnin hallinta, muutosten kontrollointi, turvallisuusasetukset, ohjelmointikäytännöt ja testaus. Elementtien järjestämisen ja toteuttamisen epäonnistuessa ohjelmistojen toiminta voi järkkyä. Viimeisenä alaluokkana oleva järjestelmien alaluokka käsittelee järjestelmien odottamatonta toimintaa, jonka riskielementteinä toimivat heikko suunnittelu, liialliset tekniset vaatimukset, huono integraatio ja monimutkaisuus. (Cebula & Young 2010)

Kolmantena kategoriana taulukossa 3 on epäonnistuneiden sisäisten prosessien kategoria. Epäonnistunut sisäinen prosessi voi johtua prosessin suunnittelun, kontrollin ja tukitoimintojen heikosta toteutuksesta. Nämä kolme muodostavat alaluokat epäonnistuneiden sisäisten prosessien kategorialle. Prosessin epäonnistuminen voi johtua muun muassa huonosti suunnitellusta prosessin kulusta, roolien ja vastuiden epäselvästä jaosta tai heikosta tehtäviensiirrosta prosessin osapuolten välillä. Prosessin kontrollien puutteellisuus voi johtaa prosessin epäonnistumiseen. Prosessin kontrollien alaluokan riskit kumpuavat epäonnistuneesta prosessin tilan valvonnasta, heikoista mittareista, jaksottaisen arvioinnin puutteesta tai prosessin

omistajuuden epäselvyyksistä. Prosessin tukitoimintojen epäonnistuminen johtuu resurssien allokoinnin puutteellisuudesta. Prosessin tukitoimintojen riskielementtejä ovat näiden resurssien toimittamiseen vaikuttavat elementit, joita ovat henkilöstöhallinta, rahoitus, koulutus- ja kehitystoiminta sekä hankinta. Resurssien puutteellinen saanti voi aiheuttaa prosessin epäonnistumisen. (Cebula & Young 2010)

Neljäs ja taulukon 3 viimeinen kategoria on ulkoiset tapahtumat. Kategoria kuvaa organisaation ulkopuolisia tapahtumia, joita organisaation ei yleensä ole mahdollista kontrolloida. Ulkopuolisten tapahtumien operationaaliset riskit on jaettu neljään alakategoriaan, joita ovat katastrofit, lainsäädännölliset ongelmat, liiketoiminnan ongelmat ja riippuvaisuussuhteet. Katastrofien alaluokka käsittää luonnonkatastrofit ja ihmisen aiheuttamat katastrofit, kuten tulvat, maanjäristykset, levottomuudet ja pandemiat. Lainsäädännölliset ongelmat voivat aiheutua esimerkiksi sääntelyn noudattamattomuudesta, organisaation toimintaan vaikuttavasta uudesta lainsäädännöstä sekä työntekijän tai osakkeenomistajan nostamasta kanteesta aiheutuvasta oikeudenkäynnistä. Liiketoiminnan ongelmien riskit muodostuvat tavarantoimittajan häiriöstä tai markkinan olosuhteista, kuten taantumasta tai organisaation omista taloudellisista olosuhteista. Ulkoisten tapahtumien viimeisenä alaluokkana ovat riippuvaisuussuhteet. Alaluokka sisältää ne riskitekijät, jotka johtuvat organisaation riippuvuudesta ulkoisista toimijoista, kuten sähkö-, vesi- ja tieliikenneverkostosta, pelastustoimesta, varavoiman saatavuudesta ja kuljetuspalveluista. (Cebula & Young 2010)

2.3 Kyberturvallisuus

Kyberriskien lisäksi jaottelua voidaan jatkaa pidemmälle puhuttaessa kybermaailman turvallisuudesta, jonka osana kyberriskit ovat. Kybermaailman turvallisuus voidaan Limnéllin ym. (2014, 105–111) mukaan jakaa haavoittuvuuksiin, uhkiin ja riskeihin. Haavoittuvuus tarkoittaa ulkoisen toimijan mahdollisuutta vaikuttaa tietojärjestelmän tieto- tai toimintavarmuuteen. Järjestelmän haavoittuvuus vaatii lähtökohtaisesti järjestelmän vian tai heikkouden sekä ulkoisen toimijan, jolla on kyky käyttää kyseistä vikaa tai heikkoutta hyväkseen. Haavoittuvuuksia ja niiden vaikutuksia voidaan hallita ja vähentää tunnistamalla ja korjaamalla niitä. (Limnell 2014, 105–111) Kyberriskiin liittyvien haavoittuvuuksien osa-alueet voidaan jakaa kahdeksaan

osaan, joita ovat organisaatio, prosessit, johtorutiinit, henkilöstö, fyysinen ympäristö, informaatiojärjestelmän konfiguraatio, laitteisto ja ohjelmisto sekä riippuvuus ulkoisista toimijoista (ISO 2018).

Uhkaksi voidaan määritellä kaikki toiminnan kannalta kielteiset asiat, jotka estävät tai vaikeuttavat toimintaa tai aiheuttavat muuta vahinkoa. Uhka voi aiheutua tahallisesti tai tahattomasti ja sen aiheuttajana voi olla niin ulkoinen kuin sisäinenkin tekijä. Uhka voidaan torjua, mutta sitä ei lähtökohtaisesti voida käsitellä muilla tavoilla. (Limnéll ym. 2014, 105–108) ENISA:n raportti (2017) luokittelee 15 tärkeintä kyberuhkaa, joita ovat haittaohjelmistot, verkkopohjaiset hyökkäykset, verkkosovellushyökkäykset, tietojenkalastelu, roskaposti, palvelunestohyökkäykset, kiristysohjelmat, tietokoneohjelmaverkot, sisäpiiriuhat, fyysinen manipulointi, tietomurrot, identiteettivarkaudet, haittaohjelman jakelualustat ja kybervakoilu.

Riskillä tarkoitetaan kaikkeen toimintaan sisältyvää epävarmuutta, jota ei voida kokonaisuudessaan torjua toimintaa jatkettaessa, mutta sitä voidaan käsitellä riskienhallinnan metodein. Uhkasta riski eroaa käsittelytavastaan, sillä uhkilta suojautumisen pääasiallinen keino on torjunta, kun taas riskit vaativat riskienhallinnallisia toimia. Kyberriski koostuu muiden riskien tapaan omaisuuden arvosta, sitä koskettavasta uhasta ja uhan realisoitumisen vaikutuksen tulosta. Näin ollen haavoittuvuudet muodostavat ja mahdollistavat uhkia ja uhat ovat osana riskejä, muodostaen kyberturvallisuuden kokonaisuuden kolmen yhteen kietoutuneen osion kautta. (Limnéll ym. 2014, 108–109)

Edellä mainittujen tekijöiden lisäksi kybermaailman turvallisuus nojaa vahvasti ihmisten luottamukseen. Mikäli luottamus kybermaailmaan tuhoutuu esimerkiksi hyökkäyksellä verkkopankkeihin, minkä seurauksena kaikki verkkopankeissa olevat rahat katoaisivat, olisi vaikeaa käyttää kybermaailmaa palveluiden tuottamiseen ja organisaation toimintaan. Luottamus toimii pohjana kybermaailman käytettävyydelle ja rakentuu kaikkien kybermaailman toimijoiden uhkien, riskien ja haavoittuvuuksien hallinnasta, jotka muodostavat yhdessä toimivan, turvallisen ja luotettavan kyberympäristön. Kyberturvallisuus koskettaa näin ollen niin yksilöitä, organisaatioita ja yhteiskuntaa kuin kaikkia muitakin maailman toimijoita, jotka käyttävät toiminnassaan teknologiaa. (Limnéll ym. 2014, 40)

2.4 Kyberriskien vaikutukset

Kyberriski voi Hamptonin (2015, 203) mukaan aiheuttaa kohteelleen tappioita monilla tavoilla, jotka voidaan jakaa neljään kategoriaan. Näitä kategorioita ovat aineelliset vahingot, aineettomat vahingot, keskeytymisvahingot ja vastuulle altistuminen. Aineelliset vahingot käsittävät kaikki ne vahingot, jotka aiheuttavat fyysisesti vahinkoa laitteistolle, toimitiloille tai muulle omaisuudelle. Hampton (2015, 203) luokittelee myös sähköverkon toiminnan aineellisen vahingon kyberriskiksi. Aineeton vahinko pitää sisällään taloudelliset vahingot aineettomalle omaisuudelle, kuten ohjelmistolle, datalle ja tietoverkoille. Yhtiön osakekurssi toimii esimerkkinä aineettomasta vahingosta. Elingin & Schnellin (2016, 478) mukaan toteutuneet kyberriskit vaikuttavat epäsuorasti listautuneiden yhtiöiden osakkeen arvoon. Yhden tapahtuneen tietomurron keskimääräinen arvioitu negatiivinen vaikutus osakkeen hintaan on noin 2,1 % tai 1,65 miljardia dollaria. Arvon laskuun vaikuttaa murron laajuus, murron kohteena olevan tiedon tärkeys ja yrityksen toiminta-ala.

Tietomurtojen negatiivinen vaikutus yrityksen arvolle aiheuttaa tilanteen, jossa suurin osa tietomurroista tai muista kyberhyökkäyksistä jätetään ilmoittamatta osakkeenomistajille. Tämä vaikeuttaa tietomurtojen ja muiden kyberriskien arviointia, joka puolestaan vaikuttaa kyberriskien vakuuttamisen mahdollisuuteen. Verrattain uuden riskin vakuutusten hinnoittelu on osoittautunut vaikeaksi, jonka vuoksi vakuutusten hinnat ja kattavuus ovat jääneet osittain heikoksi. Vakuuttamisen kustannusten ja kattavuuden heikkouden vuoksi kyberriskien vakuuttaminen on toistaiseksi hyvin maltillista. (Bandyopadhyay, Mookerjee & Rao 2009, 68–69) Yhdysvalloissa kyberriskien vakuuttaminen on yleisempää kuin Euroopassa, jossa suuri osa yrityksistä ei ole edes tietoisia kyberriskivakuutusten olemassaolosta. Osittain tämä vakuuttamisen epätasainen jakautuminen voi johtua siitä, että Yhdysvalloissa on ollut voimassa lainsäädäntöä, jonka mukaan kyberhyökkäyksistä ja tietomurroista on pakko ilmoittaa. Ilmoittamatta jättämistä on valvottu sakottamalla, minkä vuoksi tapauksista ilmoittaminen on yleistynyt Yhdysvalloissa. (Eling & Schnell 2016, 478)

Hamptonin (2015, 203–204) mukaan keskeytymisvahinkojen kategoria käsittää kaikki vahingot aineelliselle ja aineettomalle omaisuudelle, joiden avulla yritys toimii päivittäin. Vastuulle

altistumisen kategoria on kategorioista mahdollisesti suurimpia vahinkoja aiheuttava. Kattavat yhteydet verkostojen, yritysten ja toimialojen välillä sekä näiden suuri riippuvuus teknologiasta normaalin toiminnan jatkumisen edellytyksenä voi aiheuttaa toteutuneen kyberriskin kohteelle merkittäviä vastuita verkostojen muita osapuolia kohtaan. Tämä kategoria käsittää kaikki kyberriskeistä aiheutuneet vastuut niin asiakkaita kuin kolmansia osapuolia kohtaan, kuten esimerkiksi oikeuteen haastamisen ja korvausvelvollisuuden tietovuodon vuoksi. (Hampton 2015, 203–204)

Kyberriskien yhteenlasketut arvioidut kustannukset ovat vuosittain yli 100 miljardin dollarin suuruusluokassa. Arvioitu kustannus vaihtelee merkittävästi arviointitavasta riippuen ja vaihtelee 113 miljardin suorien kustannusten arviosta 445 miljardin yhteiskustannusarvioon, joka ottaa huomioon kyberriskeistä aiheutuneet epäsuorat kustannukset ja liittää ne osaksi vuosittaista kustannusarviota. Suuren epävarmuuden vallitessa arviot ovat suuntaa antavia ja painottavat pääosin riskin merkitystä, eivätkä tähtää absoluuttisen luvun arviointiin. Yksittäisen tietomurron kustannus on arvioitu keskimääräisesti 2,1 miljardin ja 3,8 miljardin dollarin välille, mikä tuo esille kyberriskien hallitsemisen tärkeyden yritykselle ja tietomurtojen määrän kokonaiskustannuksiin verrattaessa. Arviot niin kokonaiskustannuksista kuin yksittäisten tietomurtojen kustannuksista ovat kuitenkin kaukana täydellisistä arvioista ja arvioiden tekijöiden asenteellisuutta tulee tarkastella arvioita tarkasteltaessa. Laaja skaala tuo kuitenkin esille kyberriskien kokoluokkaa kustannusten näkökulmasta, joka on pienimmänkin arvion mukaan huomattava. (Eling & Schnell 2016, 477–478)

Kyberriskit voivat aiheuttaa myös yksittäisiä katastrofisia tapahtumia maantieteelliselle alueelle tai jopa koko maailmalle. Usein tarkastelupohjana on kyberriskien vaikutus organisaation toiminnalle, mutta kyberriskit koskettavat myös suurempaa yhteisöä. Laajimmillaan ne koskettavat koko sitä maailman väestönosaa, joka käyttää tietotekniikkapalveluita, kuten internetiä. Vaikka suuremman luokan kyberkatastrofit ovat kohtuullisen epätodennäköisiä, on niitä tapahtunut aiemmin ja niihin on siten syytä varautua tulevaisuudessakin. Aiemmin toteutuneita suuremman tason kyberriskejä ovat muun muassa 2013 tapahtunut vedenalaisten kaapeleiden toimintahäiriö, joka esti koko Afrikan maanosan internetin toiminnan päiväksi, sekä Etelä-Koreassa vuonna 2013 tapahtunut epäilty kyberhyökkäys, joka esti merkittävän osan maan verkkopalveluiden käytöstä. Laaja-alainen internetin toimimattomuus estäisi kommuni-

koinnin viestien, sähköpostien ja sosiaalisen median välityksellä sekä estäisi esimerkiksi verkkopankkien, tilausjärjestelmien ja verkkokauppojen toiminnan. Tämän lisäksi tapahtuma estäisi pilvipalveluiden tietoihin käsiksi pääsyn, mikä voisi aiheuttaa useiden julkisten ja yksityisten palveluiden halvaantumisen. Tällaisen kriittisen tiedon infrastruktuurin romahtamisen todennäköisyydeksi on arvioitu 10 % seuraavan vuosikymmenen aikana. Kyberriskien vaikutukset kantautuvat kaikkiin tietotekniikkaa käyttäviin ja käyttäjistä riippuvaisiin organisaatioihin, minkä vuoksi riskien toteutumisella voi olla todella suuria taloudellisia vaikutuksia. (Eling & Schnell 2016, 480–481)

2.5 Kyberriskien hallinta

Kyberriskien hallinnalla tarkoitetaan riskien tunnistamista ja arviointia, sekä riskien käsittelyä varten tehtävää vaihtoehtojen valintaa, kehittämistä ja toteuttamista. Riskienhallinta on systemaattinen ja jatkuva ajatteluprosessi, joka heijastaa organisaation arvoja. Riskienhallinta koskee kaikkia organisaatiota koskevia mahdollisia riskejä ja ongelmia niiden tapahtumista edeltävästi ja niiden tapahtumisen jälkeen. Riskienhallinta on lisäksi jatkuva toimintatapojen luomisprosessi, jolla organisaatio pyrkii välttämään ja minimoimaan riskejä ja niiden vaikutusta. Joitakin riskejä toteutuu prosessista huolimatta, jolloin riskienhallinnan tehtävänä on opettaa organisaatiota elämään toteutuvien vaikutusten kanssa. Kyberriskien hallinnassa korostuu toimijoiden joustavuus, ketteryys ja sietokyky, sillä kyberriskit eivät ole sidottuina aikaan tai tilaan eikä vastuullisuutta riskin toteutumisesta tai vahingonkorvausvelvollisuutta voida aina yksiselitteisesti osoittaa. Riskienhallinnassa uhkien katsotaan perinteisesti tulevan organisaation ulkopuolelta ja muuttuvan tunnistetuiksi riskeiksi organisaation ja maailman kohdatessa. (Limnéll ym. 2014, 109–110) Huomattavaa on, että kyberriskit ovat usein myös organisaation sisältä kumpuavia riskejä (Cebula & Young 2010).

Eling & Schnell (2016, 479–480) painottavat kyberriskien ja kyberriskien hallinnan olevan koko organisaation vastuulla eikä se näin ollen ole vain yritysten IT-osastojen tehtävänä. Kyberriskien hallitsemiseksi organisaation osastojen tulee olla tietoisia riskistä ja osallistua kyberriskien hallintaan. Organisaation osastojen kokonaisvaltaisen kyberriskien hallinnan lisäksi on

osoitettu, että kyberriskien hallinnalle oleellista on nimittää yksi henkilö vastuuseen kyberriskien hallinnasta. Kyberriskipäällikön tai vastaavan vastuullisen toimihenkilön nimittäminen alentaa keskimääräisen tietomurron kustannusta yli kolmellakymmenellä prosentilla. (Eling & Schnell 2016, 479–480)

Riskiä ei voida aina torjua vaan riski sisältyy kaikkeen toimintaan. Riskin periaatteet pätevät myös kyberriskiin. Kyberriskiä voidaan Limnéllin ym. (2014, 108) mukaan hallita välttämällä, lieventämällä, rajaamalla, siirtämällä tai omaksumalla sitä. Riskin kanssa voidaan myös niin sanotusti oppia elämään, jolloin hyväksytään valitun riskinsietokynnyksen alittavat riskitapahtumat eikä niiden välttämiseksi tehdä mitään toimenpiteitä. Riskienhallinnan kannalta tärkeää on riskitietoisuus. Riskitietoisuus muodostetaan tekemällä todennäköisyyslaskelmia ja analyysejä arvioiden tulevaisuuden negatiivisia mahdollisia tapahtumia, niiden vaikutuksia sekä todennäköisyyksiä. Riskitietoisuudella pyritään optimoimaan varautumisen aste tulevaisuuden riskeihin, sillä epätietoisuus riskeistä johtaa usein varautumisen ali- tai ylimitoittamiseen. Alimitoittaminen asettaa yhtiön toiminnan vaaraan tuntemattomien isojen riskien toteutuessa kun taas ylimitoittaminen syö resursseja yhtiön muulta toiminnalta. Tietoisuus riskien tietämättömyydestä voi taas johtaa luottamattomuuteen, jolloin yhtiö ei uskalla toimia täyden potentiaalinsa mitoissa tai välttää kannattavia toiminnan osa-alueita epävarmuuden vuoksi. Riskienhallinta on näin ollen tärkeänä komponenttina tehokkaan toiminnan kannalta. Teknologian yleistyessä riskienhallinnan merkitys korostuu yhtiölle myös kilpailuetuna, sillä kyberriskien hallinta on vielä melko uusi osa-alue ja useat yhtiöt kärsivät suuresta epätietoisuudesta kyberriskien osalta vedoten nopeaan teknologiseen kehitykseen ja yhtiön rajallisiin riskienhallintaresursseihin. (Limnéll ym. 2014, 108–109)

Riskeistä on organisaation riskienhallinnan toiminnan mahdollistamiseksi oltava olemassa mitattu arvio, jonka avulla niitä voidaan asettaa tärkeysjärjestykseen. Riskeihin pyritään tämän jälkeen vaikuttamaan ja arvioidaan vaikuttamisen tekemä lisävaikutuskyky. Organisaatiolla on mahdollisuus myös ulkoistaa osa riskeistä esimerkiksi vakuuttamistoiminnalla, jolloin riskienhallinnan tehtävänä on arvioida vakuuttamisen mahdollisuutta ja tehokkuutta sekä valita vakuutettavat riskit. Organisaation toimenpiteiden jälkeen jäljelle jääneiden riskien ja niiden mahdollisten vaikutusten kanssa on elettävä. Riskienhallinnan on arvioitava jäljelle jääneitä riskejä ja niiden vaikutuksia sekä niiden vaikutusta organisaation mahdollisuuteen jatkaa toimintaa riskien toteutuessa. Riskienhallinnan kokonaisuus koostuu näin ollen tunnistamisen,

käsittelyn ja arvioinnin lisäksi jatkuvasta koordinoinnista, riskien kehittymisen tutkimisesta, riskien uudelleen arvioinnista, korjaavista toimenpiteistä, viestinnästä sekä raportoinnista. Kyberriskeissä korostuu erityisesti riskienhallinnan näkökulmasta ajattomuus, tilattomuus ja vahingonkorvausten laskettavuuden vaikeus. Ajattomuudella viitataan päätösten vaikutukseen pitkälle tulevaisuuteen ja tilattomuudella viitataan siihen, ettei riskejä voida enää asettaa yhteen paikkaan niiden tullessa kaikkialta kansallisiin ja organisatorisiin rajoihin katsomatta. (Limnéll ym. 2014, 109–110)

Eling & Schnell (2016, 480) jakavat kyberriskien hallintaprosessin klassisesti viiteen osioon, jotka ovat kyberriskien hallinnan lähtökohdan määrittäminen ja tavoitteiden asettaminen, riskien tunnistaminen, riskien analysointi, riskienhallinta sekä riskien seuranta. Lähtökohdan määrittämistä ja tavoitteiden asettamista varten on kehitetty useita standardeja ja viitekehyksiä kuten International Organization for Standardizationin standardit (ISO 2018), joiden avulla organisaatio voi määrittää lähtökohtansa ja tavoitteensa. Riskien tunnistamista varten organisaation on keskeistä hahmottaa omaisuuserät, jotka ovat organisaatiolle erityisen tärkeitä sekä yhdistää omaisuuseriin niihin liittyvät organisaation prosessit. Kun omaisuuserät ja niihin liittyvät prosessit ovat määritelty, on organisaation mahdollista tunnistaa niihin kohdistuvat potentiaaliset uhat ja kyseisten uhkien lähteet. Tunnistamisen jälkeen riskejä voidaan analysoida eri menetelmien avulla, joista yleisenä menetelmänä toimii vaikutusanalyysi. Menetelmän avulla voidaan määrittää eri skenaarioiden arvioituja tappioita. Kyberriskien osalta menetelmän käyttö sisältää kuitenkin haasteita, sillä kyberriskit ovat luonteeltaan erittäin dynaamisia ja kyberriskien todennäköisyyksiä on vielä tällä hetkellä vaikea arvioida tiedon puutteen vuoksi. (Eling & Schnell 2016, 480–481)

Tunnistamisen ja analysoinnin jälkeen organisaatio on perinteisesti voinut hallita riskejä eri menetelmillä, joita ovat välttäminen, vähentäminen, siirtäminen sekä omalle vastuulle jättäminen. Kyberriskin välttäminen kokonaisuudessaan on useissa tapauksissa mahdotonta, sillä tällöin organisaation tulisi luopua kokonaan tietoteknologiasta. Kyberriskien vähentäminen sen sijaan on mahdollista esimerkiksi virustorjuntaohjelmilla, palomuureilla ja uusimmilla ohjelmistopäivityksillä, joilla pyritään vähentämään kyberriskien toteutumisen mahdollisuutta. Kyberriskien osalta voidaan vähentää myös toteutuneen riskin aiheuttaman tappion määrää ottamalla käyttöön esimerkiksi ohjeistus hätätilanteessa toimimiseen kyberriskin toteutuessa. Riskin siirtäminen on mahdollista vakuuttamisella, mutta vakuuttaminen on tällä hetkellä vielä

kohtuullisen pienessä osassa kyberriskien hallinnassa tiedon ja datan puutteen vuoksi. (Eling & Schnell 2016, 480)

Organisaation riskienhallinnan jatkuvuuden kannalta seuranta on tärkeässä roolissa. Kyberriskeissä riskin dynaamisuus nostaa seurannan tärkeyden erityisen korkealle, sillä kyberriskit sekä tunnettujen kyberhyökkäysten ja tietomurtojen tekotavat muuttuvat jatkuvasti aiheuttaen jatkuvan tarpeen riskienhallinnan seurannalle ja jatkotoimille. Osastojen välinen toiminta ja yhteistyö kyberriskien hallinnassa korostuvat myös seurannan näkökulmasta, sillä uusista kyberriskeistä ja tietomurtojen mahdollisuuksista on erittäin tärkeää tiedottaa koko organisaatiolle riskienhallinnan toimivuuden mahdollistamiseksi. (Eling & Schnell 2016, 480)

3 SÄÄNTELY

3.1 Sääntelyn tarkoitus ja luonne

Sääntelyllä on useita eri määritelmiä. Suosituksi on noussut Selznickin (1985, 363) määritelmä, jonka mukaan sääntely on julkisen tahon jatkuvaa ja keskitettyä valvontaa, joka keskittyy yhteisön arvostamiin aktiviteetteihin. Sääntelyn eri määritelmät tiivistyvät kuvaamaan sääntelyä tunnistettavaksi ja erotelluksi julkisen toiminnan muodoksi, mutta sääntelyä voidaan kuvailla myös monipuolisemmin jakamalla sen merkitys osiin. Sääntelyn merkitys voidaan nähdä kokoelmana käskyjä tai toimintaohjeita, tarkoituksellisena valtion vaikutusvaltana sekä talouden ja sosiaalisen vaikutusvallan kaikkina muotoina. Tässä tutkielmassa keskitytään sääntelyyn kokoelmana käskyjä tai toimintaohjeita, jolloin lakien ja sääntelyn tehtävänä on yksinomaan kieltää tai sallia asioita. (Baldwin ym. 2011, 2–3)

Sääntely voi tapahtua julkisten tahojen sijaan myös esimerkiksi organisaatioiden, ammattiliittojen, järjestöjen tai muiden ryhmien toimesta, jolloin sääntely tapahtuu usein yhteisön sisällä. Sääntelyn pääasiallisena tarkoituksena on rajoittaa toimintavaltaa tai käyttäytymistä ja estää tätä kautta ei-toivottuja tapahtumia. Laajemmin katsottuna sääntelyllä voidaan myös

mahdollistaa toimintaa järjestyksellisellä tavalla, jolloin sääntelyllä pyritään estämään vapaiden markkinoiden kaoottisuutta. Tästä esimerkkinä toimii radiolähetysten taajuuksien lupavarainen jako, jota ilman radiokanavista ei saisi selvää taajuuksien ollessa päällekkäin tai liian lähellä toisiaan. (Baldwin ym. 2011, 2–3)

Sääntelyn voidaan nähdä olevan luonnoltaan riskienhallintaa. Sääntelyn voidaan katsoa pyrkivän vaikuttamaan ensisijaisesti merkittäviin, suuriin riskeihin. Riskien tunnistamisen ja arvioinnin vaikeus tuo kuitenkin sääntelylle suuren haasteen, sillä osa riskeistä voi olla esimerkiksi odotettua suurempia tai toistumattomia ja riskien kausaalisuutta voi olla mahdotonta määrittää. Riskin sääntelyn kannalta tulee myös tarkastella sitä minkä kaltaisia riskejä halutaan torjua ja millaisia halutaan sallia. Riski voi olla esimerkiksi vapaaehtoisesti otettu tai yhteiskunnallisesti asetettu. Vapaaehtoiseen riskiin henkilö voi itse vaikuttaa, mutta yhteiskunnallisesti asetettuun riskiin, kuten ydinvoimalaan lähialueella, henkilön on vaikeampi vaikuttaa. Riskin sääntelyssä on näin ollen otettava huomioon riskin luonne ja vaikuttavuus, sekä tehtävä valintoja siitä, millaisia riskejä halutaan jättää sääntelyn ulkopuolelle ja sitä kautta ihmisten ja organisaatioiden omalle vastuulle. (Baldwin ym. 2011, 83–87)

Riskien sääntelyllä voidaan pyrkiä eri lopputuloksiin. Tällöin on tärkeää tarkastella syitä sääntelyn eroavaisuuksiin eri sääntelijöiden välillä. Riskien sääntelyssä on tunnistettavissa erilaisia näkökulmia siitä, miten riskiä tulee tarkastella ja mitata. Nämä näkökulmat toimivat lähtökohtina siihen, mihin ja miten sääntelyllä pyritään vaikuttamaan. Tällaisia näkökulmia ovat teknisen näkökulma, taloudellinen näkökulma ja psykologinen näkökulma. Teknisestä näkökulmasta katsottuna riskin määrittämisen ja sääntelyn lähtökohtana on objektiivinen analyysi valituista tilastoista. Valittua muuttujaa ja otosta, kuten kuolemia valitulla alueella, verrataan toisen alueen vastaavaan muuttujaan. Analyysin perusteella koitetaan selvittää riskejä ja riskeihin vaikuttavia muuttujia, joihin voidaan vaikuttaa sääntelyllä. (Baldwin ym. 2011, 87–88)

Taloudellinen näkökulma riskeihin muuntaa ei-toivotut vaikutukset omakohtaisiksi hyödykkeiksi siten, että eri riskien ja etujen vertailut voidaan tehdä käyttäen henkilökohtaista tyytyväisyyttä mittarina. Tämä antaa keinon liittää riskianalyysit päätösprosesseihin, joissa eri kulut ja hyödyt arvioidaan osana resurssinjakoa siten, että niiden yhteiskunnallinen hyöty maksimoidaan. Tätä näkökulmaa on käytetty erityisesti oikeudessa määritettäessä korvauksia toteutuneiden tahattomien riskien vaikutusten uhreille. Psykologinen näkökulma lähestyy riskin

mittaamista ja määrittämistä yksilön näkökulmasta keskittyen siihen miten yksilö kokee riskin. Yksilö voi käyttäytyä epäloogisesti riskitilanteissa riippuen riskin luonteesta. Olemassa olevan riskin ja yksilön kokeman riskin eroavaisuudet voivat johtua esimerkiksi riskin tunnettuudesta, vapaaehtoisuudesta riskinottotilanteessa tai riskin katastrofaalisesta luonteesta. (Baldwin ym. 2011, 88–89)

Riskiä ei siis koeta loogisella tavalla vaan siihen vaikuttaa yksilön omat uskomukset, joista Baldwin ym. (2011, 90) nostavat esimerkiksi maanjäristysvakuutuksen. Maanjäristysvakuutus ostetaan todennäköisimmin maanjäristyksen jälkeen, jolloin maanjäristyksen todennäköisyys on pienempi kuin aikana, jolloin viime maanjäristyksestä on jo aikaa. Näiden näkökulmien lisäksi esiin on nostettu kulttuurinen näkökulma, jonka mukaan kulttuurin sisällä jaetut uskomukset ja asenteet vaikuttavat siihen millaiseksi riski koetaan. Kulttuurin vaikutukset voivat sekä vahvistaa että lieventää koettua riskiä. (Baldwin ym. 2011, 87–92)

Eri näkökulmat vaikuttavat siihen, miten lakeja ja sääntelyä muodostetaan ja mitä asioita sääntelyllä halutaan saavuttaa. Aiemmin mainitut näkökulmat ovat tärkeitä huomioida sääntelyä tarkastellessa ja nostavat esiin mahdollisia ongelmia sääntelystä, mikäli näkökulmat vaikuttavat sääntelyn luomiseen. Korkea luottamus tekniseen näkökulmaan sääntelyn osalta johtaa riskien sääntelyn jättämiseen ammattilaisten tehtäväksi, jolloin sääntelyn kohteiksi priorisoituvat teknisen sääntelyn mukaiset kohteet. Mikäli taas luotetaan riskien psykologiseen näkökulmaan, saattaa sääntelyn objektiivinen suhtautuminen riskeihin vähentyä, joka voi johtaa epäloogiseen sääntelyyn riskien näkökulmasta. (Baldwin ym. 2011, 92–93) Sääntely ei voi myöskään pyrkiä pelkästään maksimoimaan taloudellista vaurautta, sillä vaurauden maksimointi voisi johtaa eettisesti katsottuna epäoikeudenmukaisiin ratkaisuihin sääntelyä tehdessä ja sovellettaessa. (Baldwin ym. 2011, 25)

3.2 Hyvä sääntely

Mikä tekee sääntelystä hyvää? Lähtökohtana hyvälle sääntelylle on oikeusnormien tunnusmerkkien täyttäminen. Sakari Wuolijoen (2016, 2) mukaan:

> *”Oikeusvaltiossa esimerkiksi edellytetään, että normit ovat luonteeltaan yleisiä eivätkä koske vain yksittäistapauksia. Oikeusvaltion toiminnan perusedellytyksistä voidaan johtaa myös sääntelyn määrään liittyviä vaatimuksia. Jotta demokraattinen oikeusvaltio toimisi, sääntelyä on oltava tietty vähimmäismäärä. Jos normeja olisi kovin vähän tai ne olisivat aivan yleisluontoisia, valta siirtyisi käytännössä tuomareille ja muille lain tulkintavirkamiehille, mikä olisi jo vallanjako-oppienkin näkökulmasta ongelmallista.” (Wuolijoki 2016, 2)*

Myös liian laaja sääntely tai sen jatkuva muuttuminen on oikeusturvan kannalta kestämätöntä, sillä se estää sääntelyn selvyyden ja selonoton. (Wuolijoki 2016, 2)

Sääntelyn hyvyyttä on vaikea tarkastella absoluuttisesti, minkä vuoksi sitä täytyy tarkastella eri näkökulmien avulla. Yhteiskunnan kannalta Wuolijoki (2016, 2) nostaa merkityksellisimmäksi sisällön onnistuneisuuden sääntelyssä. Sisällön onnistuneisuudella tarkoitetaan sitä, että sääntely keskittyy hyviin tarkoitusperiin ja niiden toteuttamiseen. Ongelmana on kuitenkin se, ettei sääntelyn aineellista sisältöä tai tavoitteita voida arvioida yksiselitteisesti. Hyvän sääntelyn periaatteilla tarkoitetaan yleisesti ”…toimintatapoja, joilla lainsäädäntö valmistellaan laadukkaasti, ja lainsäädännön muodollista laadukkuutta. Hyvään sääntelyyn tässä mielessä voidaan katsoa kuuluvan myös sääntelyn perustuslainmukaisuus ja sen yhteensopivuus kansainvälisten velvoitteiden kanssa. Yksiselitteisiä tai normatiivisesti määriteltyjä kriteerejä hyvän sääntelyn periaatteiden sisällöstä ei kuitenkaan ole.” (Wuolijoki 2016, 2)

Hyvänä pidettävään lainvalmistelun prosessiin liittyvät sääntelyn taloudellinen vaikutusarviointi, sidosryhmien kuuleminen, eri vaihtoehtojen arviointi, ennakoitavuus ja avoimuus. Hyvän lainvalmisteluprosessin kuuluu Wuolijoen mukaan (2016, 2) noudattaa päätöksentekoa, jossa edetään ”ongelman tunnistamisesta ja tavoitteenasettelusta eri vaihtoehtojen punninnan kautta parhaan sääntelymallin valintaan.” Tätä kutsutaan rationaaliseksi päätöksentekomalliksi. Sisällön osalta sääntelylle tärkeää ovat johdonmukaisuus, yksinkertaisuus, helppo tulkittavuus sekä sovellettavuus. Sääntelyä pitää pystyä myös valvomaan helposti. (Wuolijoki 2016, 2)

Hyvää sääntelyä on siis käytännössä mahdotonta vahvistaa yksiselitteisesti, minkä vuoksi sääntelyyn ja sen toimivuuteen liittyy aina kiistanalaisuutta. Baldwinin ym. (2011, 26–32) mu-

kaan hyvälle sääntelylle voidaan asettaa viisi kriteeriä, jotka ovat lainsäädäntöelimen toimeksianto, vastuuvelvollisuus, oikeudenmukainen prosessi, asiantuntemus ja tehokkuus. Lainsäädäntöelimen toimeksiannolla sääntelytoimen oikeellisuus perustuu sen hyväksyntään lainsäädäntöelimen, kuten eduskunnan tai parlamentin toimesta. Taustalla toimeksiannossa on usein tilanne, jossa lainsäädäntöelin antaa sääntelijän tehtäväksi saavuttaa haluttu tilanne sääntelyllä. Annetun tehtävän toteutuessa sääntelijän voidaan nähdä onnistuneen tehtävässään ja sääntelyn olevan hyvää. Ongelmallisena toimeksiannoissa voidaan nähdä niiden tulkinnallisuus, jolloin saavutettavat asiat jäävät tulkinnanvaraisiksi. Toimeksiannot voivat myös vaikuttaa toiseen osapuoleen asiaa etukäteen huomaamatta. Esimerkiksi tilanteessa, jossa sääntelyllä halutaan parantaa kuluttajan asemaa, voi sääntely vaikuttaa negatiivisesti teollisuuteen. (Baldwin ym. 2011, 27–28)

Vastuuvelvollisuudella viitataan siihen, että sääntelijän tai sääntelyn toteuttajan tulee olla velvollisuudessa vastuustansa, jotta sääntely ja sen toteutus voivat toimia. Oikeudenmukainen prosessi ottaa huomioon sääntelyn prosessin, joka tulee olla reilu, avoin ja helposti saatavissa. Toimilla voidaan varmistaa, että sääntelyn tekovaihe ottaa huomioon tasa-arvon, oikeudenmukaisuuden ja johdonmukaisuuden, sekä huomioi sääntelyn vastaanottavan osapuolen prosessissa. Asiantuntemukseen voidaan viitata muiden selitysten sijaan, mikäli kritiikkiä kohdataan sääntelytehtävissä. Asiantuntijataho voi tällöin vakuuttaa päätyvänsä nopeasti parhaaseen mahdolliseen lopputulokseen silloin kun selityksiä valituille sääntelytoimille ei tarvitse antaa. Ongelmana asiantuntemukseen viitatessa on sen läpinäkymättömyys, jolloin päätöksiä ei voida julkisesti tarkastella ilman selityksiä. Asiantuntijuus on tämän vuoksi oltava varmistettavissa hyvän sääntelyn saavuttamiseksi. Tehokkuus on sääntelylle tärkeää julkisen hyväksynnän saamiseksi. Ongelmana näkökulmassa on tehokkuuden arviointi, joka on usein hyvin vaikeaa. (Baldwin ym. 2011, 27–31)

3.3 Kaupallisen siviili-ilmailun sääntely

Ilmailu on hyvin kansainvälinen ala, minkä vuoksi ilmailualan sääntelyn on oltava kansainvälisesti yhteensopivaa. Kansainvälisyys korostaa valtioiden ja alueiden yhteisiä sopimuksia ja sääntöjä, joita ilman ilmailua olisi hankala toteuttaa. Ilmailualalla toimii useita järjestöjä, jotka

antavat normeja ilmailuun sekä harjoittavat kansainvälistä yhteistyötä. Esimerkkejä kansainvälisistä sopimuksista ovat Kansainvälisen siviili-ilmailun yleissopimus, Sopimus kauttakulusta kansainvälisessä lentoliikenteessä, Lennonvalmistusalan yhteistyöstä tehty kansainvälinen yleissopimus ja navigaatiomaksuja koskeva monenvälinen sopimus sekä Sopimus eräiden kansainvälistä ilmakuljetusta koskevien sääntöjen yhtäläistyttämisestä. (Trafi 2018a) Tämä tutkielma on rajattu käsittelemään ilmailualan normeja, standardeja, lakeja ja muuta sääntelyä vain Euroopan sekä siviili-ilmailun näkökulmasta.

Euroopan unionin lainsäädäntötyö on Trafin (2018b) mukaan edennyt niin laajalle, että kansallisen lainsäädännön merkitys on jatkuvasti vähentynyt. Euroopan unionin asetukset ovat Suomessa voimassa sellaisenaan. Euroopan unionissa lainsäädäntövalta on jakautunut Euroopan parlamentille ja Euroopan unionin neuvostolle. Tämän lisäksi Euroopan unionissa toimii toimielimenä Euroopan komissio ja strategisena toimielimenä Eurooppa-neuvosto. Euroopan parlamentti on unionin ainut vaaleilla valittu toimielin, jossa jäsenmaiden mepit edustavat unionin kansalaisia. Euroopan unionin neuvosto koostuu jäsenmaiden hallitusten ministereistä. Neuvosto jakaa lainsäädäntövallan lisäksi budjettisäädäntövallan Euroopan parlamentin kanssa. Euroopan komissio on Euroopan unionin (2018a) mukaan ”…EU:n poliittisesti riippumaton toimeenpanoelin. Se tekee lainsäädäntöehdotuksia ja vastaa Euroopan parlamentin ja EU:n neuvoston päätösten täytäntöönpanosta.” Tämän lisäksi ”Komissio on ainoa EU:n toimielin, joka voi esittää lainsäädäntöä Euroopan parlamentin ja neuvoston hyväksyttäväksi.” Eurooppa-neuvosto päättää strategisena toimielimenä unionin suurista poliittisista linjoista ja sitä edustavat unionin jäsenmaiden päämiehet. (Euroopan unioni 2018a)

3.3.1 Euroopan unionin sääntelyn laajentuminen

Euroopan parlamentin ja Euroopan unionin neuvoston asettama lainsäädäntö keskittyy turvaamaan ja yhtenäistämään ilmailualan turvallisuutta sekä matkustajaturvallisuutta. Ilman tiukkaa sääntelyä siviili-ilmailu ei olisi voinut kehittyä nykyiseen muotoonsa, minkä vuoksi siviili-ilmailun sääntely on koettu Euroopan unionin osalta tärkeäksi. Euroopan unionin lainsäädäntö noudattaa Kansainvälisen siviili-ilmailujärjestön standardeja, mutta on usein standardeja tiukempaa. Sääntelyä on asteittain laajennettu koskemaan kaikkia ilmailualan sektoreita onnettomuuksien välttämiseksi. Euroopan unionin sääntely ja järjestelmä siviili-ilmailussa on

korvannut aikaisemmin useiden maiden yhteisenä toimielimenä toimineen Joint Aviation Authoritiesin. Nykyinen Euroopan unionin järjestelmä yhdistää kansallisten auktoriteettien, Euroopan komission ja Euroopan lentoturvallisuusviraston toiminnat yhdeksi toisiinsa liittyväksi kokonaisuudeksi. (Euroopan parlamentti 2018)

Sääntely on laajentunut asteittain alkaen Euroopan unionin lainsäädännöstä, joka asetti vuonna 1994 direktiivin siviili-ilmailun onnettomuuksien tutkinnalle. Direktiivin mukaan tutkinnan tulee olla täysin itsenäinen, keskittyä etsimään onnettomuuden syy ja estämään onnettomuuksia tulevaisuudessa, eikä keskittyä etsimään syyllistä tai kohdistamaan syyllisyyttä. Direktiivi erosi joidenkin jäsenvaltioiden aikaisemmasta omasta lainsäädännöstä, jossa syyllisen tuomitseminen oli keskiössä. Euroopan unioni on sittemmin korvannut direktiivin uudistetulla sääntelyllä 2010. Tämän lisäksi unioni on luonut direktiivejä ja lakeja ongelmien raportoimisesta siviili-ilmailussa vuosina 2003 ja 2007. Nämä direktiivit ovat luonteeltaan yhtälailla ongelmiin keskittyviä syyllisyyskeskeisyyden sijaan. Sääntelyn mukaan ongelmista tuli raportoida kansallisen viranomaisen toimesta Euroopan lentoturvallisuusvirastolle vuodesta 2005 alkaen, jonka jälkeen virasto varastoi ja analysoi raportit. Vuodesta 2003 alkaen unionin perussäännöt ovat asettaneet vaatimuksia myös ilmakelpoisuudelle ja vuonna 2008 unionin sääntely ulotettiin koskemaan myös lentotoimintaa ja miehistön koulutusta. Vuonna 2009 sääntelyä laajennettiin säätelemään lentokenttien, lennonjohdon ja lennonvarmistuspalveluiden toimintaa. Sääntely koskee myös Euroopan unionin ulkopuolisista maista käsin Euroopassa toimivien yhtiöiden osalta kaikkia lentokoneita, lentokoneiden osia, organisaatioita, lentokoneiden suunnittelijoita ja huoltajia sekä lentäjiä. Lisäksi vuodesta 2016 alkaen kaikkien toimijoiden, jotka haluavat lentää Euroopan unionin alueelle, on tullut osoittaa toimivansa Kansainvälisen siviili-ilmailujärjestön turvallisuusvaatimusten mukaisesti. Euroopan lentoturvallisuusvirasto auktorisoi vaatimukset täyttävät toimijat. (Euroopan parlamentti 2018)

Mikäli Euroopan unionin vaatimuksia ei täytetä, voi toimija joutua niin kutsutulle mustalle listalle estäen toiminnan Euroopan unionin alueella. Euroopan unioni toimii yhdessä Kansainvälisen siviili-ilmailujärjestön kanssa auttaakseen maita, joiden on todettu olevan suurimmissa vaikeuksissa tehokkaiden turvallisuussysteemien turvaamiseksi. Tämän lisäksi Euroopan unioni on kehottanut unionin lähellä olevia maita ja suosittuja matkustuskohteita liittymään alueen sääntelyn alaisuuteen siirtymällä niin kutsutuille sisäisille lentomarkkinoille. Maiden tulisi tällöin hyväksyä ja implementoida Euroopan unionin turvallisuussääntely ilmailun osalta.

Ilmailualan kannalta tärkeimpien unionin sääntelyn ulkopuolisten maiden kanssa on myös tehty turvallisuuden vastavuoroista tunnustamista koskevia sopimuksia, jotta sopimusten alaisia tuotteita ja palveluita voidaan vaihtaa vapaasti. Näitä maita ovat Yhdysvallat, Kanada ja Brasilia. Tämän lisäksi Euroopan lentoturvallisuusvirasto on tehnyt projektikohtaisia sopimuksia tärkeiden teollisuusmaiden kanssa, jotka eivät kuulu vastavuoroisen tunnustamisen sopimuspiiriin. (Euroopan parlamentti 2018)

Euroopan komissio on vuodesta 2002 lähtien asettanut siviili-ilmailulle yleisiä matkustajaturvan sääntöjä, joilla pyritään suojelemaan ihmisiä ja tavaroita laittomalta häirinnältä. Euroopan parlamentti ja neuvosto ovat asettaneet yleiset perussäännöt ja -standardit ilmailun turvallisuudelle sekä asettaneet menettelytavat sääntöjen ja standardien implementoinnin valvomiseksi asetuksella N°300/2008. Asetus korvasi aikaisemman, vuonna 2002 tehdyn asetuksen, joka korvattiin uudella asetuksella kehittyvien riskien vuoksi sekä uuden teknologian käyttöönoton mahdollistamiseksi. (Euroopan komissio 2018a)

Yleiset perusstandardit käsittävät matkustajien ja matkatavaroiden seulonnan, lentokentän turvallisuuden ja valvonnan, lentokoneiden turvallisuustarkastukset ja -etsinnät, rahdin ja postin seulonnan, lentoaseman tarvikkeiden seulonnan sekä henkilöstön rekrytoinnin ja kouluttamisen. Perusstandardien mukaan jäsenvaltioiden tulee huolehtia siitä, että ne nimeävät yhden pätevän auktoriteetin ilmailun turvallisuudelle, järjestävät kansallisen siviili-ilmailun turvallisuusohjelman ja järjestävät kansallisen laadunvalvonnan ohjelman. Lentoliikenteen toimijoiden tulee perusstandardien mukaan määrittää ja implementoida lentokenttäturvallisuusohjelma ja lentoliikenteen harjoittajan turvallisuusohjelma. Euroopan komissio tarkensi implementaatiolakeja vuonna 2016, jolloin implementointisääntöjä muutettiin yksityiskohtaisemmiksi. Euroopan komissiolla on myös peruslainsäädäntö komission tarkastusten suorittamisesta ilmailualalla. (Euroopan komissio 2018a)

3.3.2 Kansalliset sääntelijät

Trafin (2018b) mukaan kansallisen sääntelyn merkitys on jatkuvasti vähentynyt Eurooppalaisessa ilmailussa Euroopan unionin keskitetyn lainsäädäntötyön, asetusten ja vaikutusten vuoksi. Suomessa kansallinen lainsäädäntö on asetettu pääosin Euroopan unionin direktiivien

vahvistamiseksi. Sen lisäksi suomalainen ilmailulaki (Ilmailulaki 7.11.2014/864) osoittaa toimivaltaiset viranomaiset esimerkiksi Euroopan unionin antamien maahuolintadirektiivin, puiteasetuksen, palveluntarjonta-asetuksen ja yhteentoimivuusasetuksen osalta. Suomen osalta toimivaltainen viranomainen on Liikenteen turvallisuusvirasto Trafi. (Trafi 2018b)

Euroopan unionin sääntelyn vuoksi kansallisten ilmailuviranomaisten vastuulle ovat jääneet enää sotilas-, tulli- ja poliisitehtävien lentotoiminta, ilmaliikenteen hallinta, lennonvarmistuspalvelut, puolustusvoimien valvonnassa olevat lentopaikat sekä vähäisessä käytössä olevat yksityislentokentät. Kansalliset ilmailuviranomaiset vastaavat maansa liikennöintilupien myöntämisestä. Jäsenvaltioiden kansalliset viranomaiset vastaavat myös lentoturvallisuuden varmistamisesta omalla alueellaan, niin maassa kuin ilmatilassa. Kansallisten viranomaisten tehtävänä ovat näiden lisäksi esimerkiksi jäsenmaan organisaatioiden hyväksyntä, henkilöstön lupakirjat ja kansallinen valvonta. (Euroopan Komissio 2015a) Kansallisten ilmailuviranomaisten on käytettävä Euroopan lentoturvallisuusviraston antamia proseduureja ja Euroopan unionin asettamia implementointisäädöksiä. (FAA 2012)

Siviili-ilmailun osalta Euroopan lentoturvallisuusvirasto on vastuussa kaikkien jäsenmaiden lentokoneiden ja tuotteiden sertifioinnista ja valvonnasta. Sertifioinnista ja valvonnasta poikkeavat vain erikseen mainitut tuotteet, joita ovat esimerkiksi ultrakevyet lentokoneet ja historialliset lentokoneet, jotka jäävät kansallisten ilmailuviranomaisten valvottavaksi. Kaikki yleisesti käytettävät siviili-ilmailun lentokoneet jäävät näin ollen Euroopan lentoturvallisuusviraston vastuulle. (FAA 2012) Jäsenvaltioiden kansalliset viranomaiset ovat vastuussa kansallisen turvallisuusohjelman laatimisesta, jonka tulee täyttää Kansainvälisen siviili-ilmailujärjestön standardit sekä oltava linjassa Euroopan lentoturvallisuusohjelman kanssa. (Euroopan komissio 2015a)

3.3.3 Järjestöt, organisaatiot ja virastot

Ilmailualan järjestöjen tehtävät eroavat toisistaan ja niitä on maailmanlaajuisesti monia. Niin kutsuttuna kattojärjestönä toimii Yhdistyneiden kansakuntien erikoisjärjestö International Civil Aviation Organization, jota kutsutaan Suomessa Kansainväliseksi siviili-ilmailujärjestöksi

(Trafi 2018c). Kansainvälinen siviili-ilmailujärjestö on vuonna 1944 Kansainvälisen siviili-ilmailun yleissopimuksella perustettu järjestö, johon kuuluu 192 jäsenvaltiota. (ICAO 2018b) Yleissopimuksen allekirjoittaneet valtiot hyväksyivät sopimuksen osaksi lainsäädäntöään. Sopimus määrittää esimerkiksi jokaisen valtion yksinomaisen herruuden ilmatilaansa, kieltoalueoikeudet valtion ilmatilalle sekä oikeuden maahantulo- ja selvitysmääräyksiin. Tämän lisäksi sopimus rajoittaa esimerkiksi ilma-aluksen rekisteröinnin vain yhteen valtioon ja sitoo sopimusvaltioita muun muassa hädässä olevien ilma-alusten auttamiseen. (Kansainvälisen siviili-ilmailun yleissopimus 1949/11)

Kansainvälisen siviili-ilmailujärjestön tehtävänä on kehittää kansainvälisiä siviili-ilmailun standardeja ja suositeltuja käytäntöjä, jotka auttavat luomaan tehokasta, turvallista, varmaa ja taloudellisesti sekä ympäristöllisesti vastuullista siviili-ilmailusektoria. Jäsenvaltiot kehittävät lainsäädäntöään järjestön antamien standardien ja suositeltujen käytäntöjen mukaan. (ICAO 2018b) Jäsenvaltiot voivat kuitenkin poiketa annetuista standardeista ja suositelluista käytännöistä ja jättää ne vahvistamatta omaan lainsäädäntöönsä. Tällöin poikkeuksista tulee ilmoittaa järjestölle, minkä jälkeen järjestö julkaisee poikkeukset kansainvälisesti tarkasteltavaksi. (ICAO 2018c) Tällä koetetaan ohjata jäsenvaltioita pysymään standardeissa, mikäli poikkeustarvetta ei erityisestä syystä ole.

Standardien ja suositeltujen käytäntöjen lisäksi Kansainvälinen siviili-ilmailujärjestö koordinoi valtioiden avustamista ja valmiuksien kehittämistä jäsenvaltioiden ilmailun kehittämistavoitteiden tukemiseksi sekä tuottaa maailmanlaajuisia suunnitelmia ilmaturvallisuuden ja -navigoinnin kehittämiseksi. Järjestö myös valvoo ja raportoi lukuisista lentoliikennesektorin suorituskyvyn mittareista sekä tarkastelee valtioiden siviili-ilmailun valvontavalmiuksia turvallisuuden ja varmuuden alueilla. Järjestön tehtävänä on siis pääosin raportointi ja tiedotus sekä lainsäädännön yhtenäistämisen suosittelu standardien avulla. (ICAO 2018b)

Euroopassa lentoturvallisuusvirastona toimii vuonna 2002 perustettu European Aviation Safety Agency. Virasto vastaa Euroopan lentoliikenteen turvallisuuden ja ympäristönsuojelun varmistamisesta sekä sille annetuista auktorisointitehtävistä (Euroopan unioni 2018). Euroopan lentoturvallisuusvirastolla korvattiin vuonna 1970 perustettu Joint Aviation Authorities, jonka toiminta siirrettiin vuodesta 2003 alkaen asteittain Euroopan lentoturvallisuusvirastolle (JAATO 2018a). Euroopan lentoturvallisuusvirastoon kuuluvat kaikki Euroopan unionin maat

sekä Sveitsi, Norja, Islanti ja Liechtenstein. Viraston tehtäviin kuuluvat ”…sääntelyn ja sertifioinnin yhdenmukaistaminen, EU:n ilmailualan sisämarkkinoiden kehittäminen, ilmailutoiminnan teknisten sääntöjen laatiminen, ilma-alusten ja niiden komponenttien tyyppihyväksyntä, ilmailutuotteita suunnittelevien, valmistavien ja huoltavien yritysten hyväksyntä, ilmailun turvallisuusvalvonta ja turvallisuuteen liittyvä tuki EU-maille (esim. lentotoiminta, ilmaliikenteen hallinta), eurooppalaisten ja maailmanlaajuisten turvallisuusstandardien edistäminen…” sekä ”…yhteistyö kansainvälisten sidosryhmien kanssa turvallisuuden parantamiseksi Euroopassa (esim. ns. musta lista, joka sisältää kaikki EU:ssa kielletyt lentoyhtiöt).” (Euroopan unioni 2018a)

Euroopan lentoturvallisuusvirasto kerää, tutkii ja analysoi tietoa lentoturvallisuuden parantamiseksi. ”Tässä työssä sitä tukevat ilmailualan turvallisuusanalyytikkojen verkosto (NoA), Euroopan kaupallisen lentotoiminnan turvallisuusryhmä (ECAST), Euroopan helikopteriturvallisuusryhmä (EHEST) ja Euroopan yleisilmailun turvallisuusryhmä (EGAST).” Lisäksi Euroopan lentoturvallisuusvirastolla ”…on valtuudet antaa hyväksyntöjä kolmansien maiden kaupallisille lentotoiminnan harjoittajille, jotka liikennöivät 28 EU-jäsenvaltion tai EFTA-maiden (Islanti, Norja, Liechtenstein ja Sveitsi) alueelle, alueella tai alueelta.” Euroopan lentoturvallisuusvirasto ”…huolehtii ainoastaan ulkomaisten lentoliikenteen harjoittajien arvioinnin turvallisuuteen liittyvästä osasta.” Virasto vastaa myös Euroopan lentoturvallisuussuunnitelman laatimisesta ja hyväksymisestä sekä Euroopan ilmailun alalla tapahtuvan verkkokriisin toimien hallinnan koordinoinnista. (Euroopan komissio 2015a)

Euroopan lentoturvallisuusvirasto muodostuu viidestä eri osastosta, joita ovat hallinto, strategia ja turvallisuuden hallinta, sertifiointi, lentostandardit sekä resurssit ja tuki (Euroopan unioni 2018b). Euroopan lentoturvallisuusviraston hallitusneuvosto koostuu Euroopan komission ja jäsenvaltioiden edustajista. Hallitusneuvosto laatii viraston työohjelman, valvoo viraston toimintaa ja vahvistaa viraston talousarvion. (Euroopan komissio 2015a) Euroopan lentoturvallisuusviraston tarkoituksena on yksinkertaistaa Euroopan ilmailun sääntelyä ja toimia yksittäisenä erikoistuneena asiantuntijatoimielimenä, joka tarjoaa asiantuntijuutta Euroopan unionille lainvalmistelun ja lakien implementoinnin osalta. Virasto on riippumaton teknisistä asioista ja sillä on taloudellinen, hallinnollinen ja oikeudellinen itsemääräämisoikeus. Virasto ei kuitenkaan voi antaa oikeudellisesti sitovia tulkintoja EU-sääntelystä. Sitovista tulkinnoista vastaavat Euroopan unionin omat tuomioistuimet, kansalliset tuomioistuimet sekä Euroopan

komissio. Virasto auttaa laatimaan Euroopan unionin lainsäädäntöä, minkä jälkeen Euroopan parlamentti päättää lainsäädännön hyväksymisestä, ehdotuksen muuttamisesta tai ehdotuksen hylkäämisestä. Euroopan unionin jäsenvaltiot ovat perussopimusten mukaan vastuussa unionin asettamien lakien tulkinnasta ja voimaansaattamisesta kansalliseen lainsäädäntöönsä. Euroopan lentoturvallisuusviraston toiminta ei ulotu kansalliseen viranomaistoimintaan, kuten armeijan, tullin tai poliisin toimintaan jäsenvaltioissa. (EASA 2018b)

Eurooppalaisen ilmailun tukena toimii myös lennonjohtoasioihin keskittyvä European Organisation for the Safety of Air Navigation, joka tunnetaan yleisesti nimellä EUROCONTROL. Organisaation jäseninä on 41 valtiota, sisältäen tällä hetkellä myös kaikki Euroopan unionin maat. Organisaatio ei ole Euroopan unionin virasto kuten Kansainvälinen ilmailuvirasto on, vaan se toimii ulkoisena organisaationa, joka keskittyy lennonjohtotoimien yhtenäistämiseen ja turvallisuuteen. (EUROCONTROL 2018a) Organisaation tehtävänä on auttaa jäsenvaltioitaan suorittamaan turvallista, tehokasta ja ympäristöystävällistä lennonjohtotoimintaa Euroopan alueella. Organisaatio toimittaa lennonjohtoverkkoa Euroopan alueella läheisessä yhteistyössä palveluntuottajien kanssa, toimii Hollannin, Belgian, Luxemburgin ja Saksan lennonjohtojärjestelmien toimittajana, kerää jäseniltään maksuja sekä osallistuu tutkimus-, kehittämis- ja validointitoimintaan lennonjohtojärjestelmien parantamiseksi. Tällä hetkellä organisaation tehtävänä on myös auttaa Euroopan unionia suorittamaan sääntelyuudistusta, josta käytetään nimitystä Single European Sky. Sääntelyuudistus keskittyy yhtenäistämään Euroopan alueen ilmailualaa lennonjohtamisen ja ilmailun näkökulmista, minkä tekemisessä organisaatio toimii neuvovana osapuolena lennonjohtotoimien näkökulmasta. (EUROCONTROL 2018b)

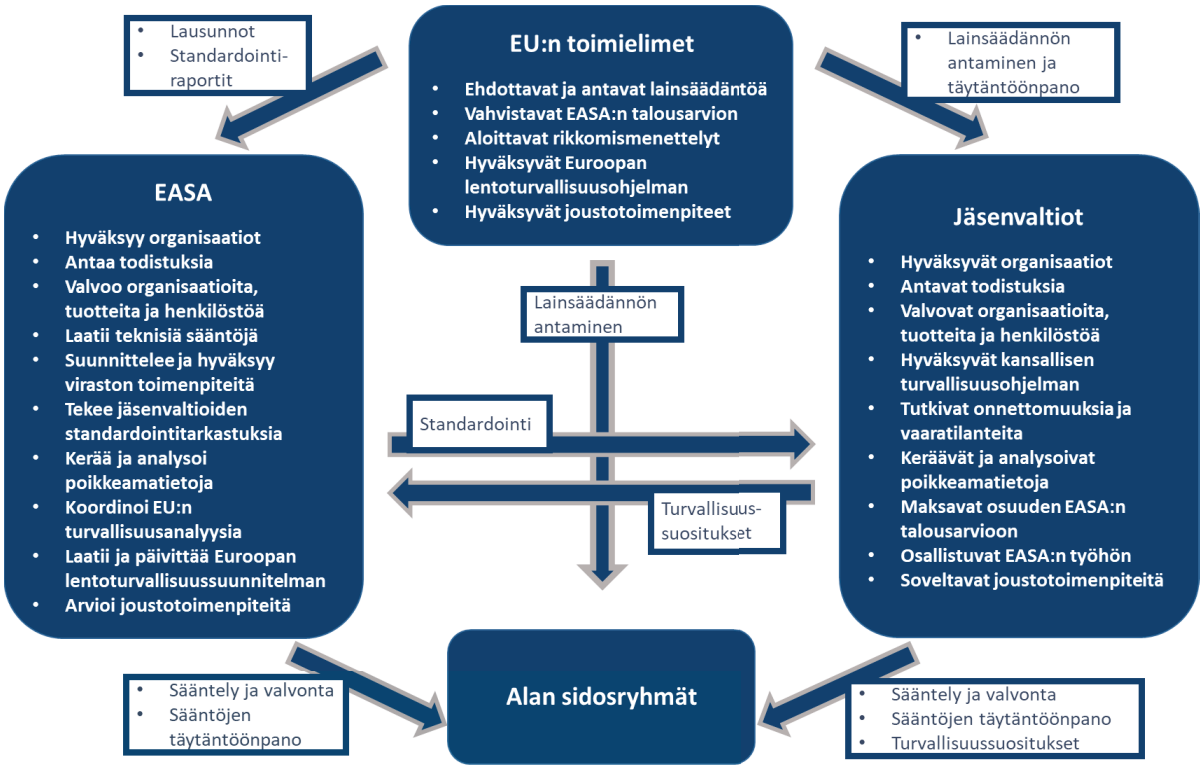
Lentoyhtiöiden liittoumana toimiva The International Air Transport Association edustaa sen jäseninä olevia lentoyhtiöitä, joita on tällä hetkellä noin 290. Järjestön mukaan jäsenet kattavat 82 % maailman lentoliikenneyhtiöistä. Järjestön tehtävänä on tukea ilmailua lentoyhtiöiden näkökulmasta ja auttaa muotoilemaan alan kriittisiä käytäntöjä. (IATA 2018a) Järjestön tarkoituksena on edustaa, johtaa ja palvella lentoliikennealaa sekä keskittyä arvonluontiin, turvallisuuteen ja ilmailualan kannattavuuteen. Tämän lisäksi järjestö ajaa ilmailualan vastuullisuutta. Edustamistoiminnassa järjestö tuo päättäjien tietoon lentoyhtiöiden näkökulmaa, lisää tietoisuutta lentokuljetuksen alasta, ajaa lentoyhtiöiden puolta haastamalla kohtuuttomia sääntöjä ja kuluja sekä pitää huolen sääntelijöiden ja hallitusten vastuista ilmailualaa kohtaan. Ilmailualan johtamiseksi järjestö on kehittänyt kaupallisia standardeja toiminnan tukemiseksi.

Järjestö tarjoaa myös ammattilaisapua alan toimiojille. (IATA 2018b) Tällä hetkellä järjestön prioriteetteihin kuuluu muun muassa lentokenttä- ja polttoainekustannusten pienentäminen sekä järjestön matkatavaroiden standardin ”Resolution 753”:n implementointi jäsenyhtiöiden toimintaan. Tämän lisäksi järjestö keskittyy tällä hetkellä tarjoamansa turvallisuustarkastuksen tunnustuksen lisäämiseen sääntelymuutoksia ajamalla kuudessa eri maassa. (IATA 2018c)

European Civil Aviation Conference on vuonna 1955 perustettu hallitustenvälinen järjestö (ECAC 2018a), jonka jäseninä ovat 44 valtiota mukaan lukien kaikki Euroopan Unionin jäsenvaltiot (ECAC 2018b). Järjestön tehtävänä on harmonisoida siviili-ilmailun politiikkaa ja käytäntöjä. Tämän lisäksi järjestö listaa tehtäväkseen turvallisen, tehokkaan ja kestävän Eurooppalaisen lentoliikennejärjestelmän jatkuvan kehittämisen. Järjestö toimii yhteistyössä muun muassa Kansainvälisen siviili-ilmailujärjestön, Euroopan komission ja EUROCONTROLin kanssa. Järjestön jäsenvaltiot voivat käyttää järjestöä keskustelualustana siviili-ilmailun kriittisiä asioita varten. Tämän lisäksi järjestö järjestää tasaisin väliajoin kansainvälisiä symposiumeja, seminaareja ja koulutustapahtumia jäsenvaltioilleen. (ECAC 2018a)

3.3.4 Eri toimijoiden välinen vuorovaikutus Euroopassa

Sivulla 44 esitetty kuvio 3 on mukaillen uudelleentehty vuorovaikutuskaavio, joka perustuu yksityiskohtaisesti Euroopan komission julkaisemaan kaavioon. Euroopan lentoturvallisuuden varmistaminen toimii kaikkien Euroopan ja kansallisten toimijoiden yhteistoimintana. Yhteistyö voi olla hankalasti hahmotettavaa useiden toimijoiden ja vastuunjakojen vuoksi. Kuvio 3 osoittaa yhteistyön pääpiirteet. Kuvion mukaan Euroopan unionin toimielimet tekevät lainsäädännön, joka annetaan jäsenmaille toimeenpantavaksi. Euroopan lentoturvallisuusvirasto on Euroopan unionin nimittämä virasto, jonka tehtävänä on Kuviossa 3 osoitettujen toimenpiteiden toimittaminen. Virasto auttaa Euroopan unionia laatimaan lakeja lakiehdotuksilla sekä laatii ja toimittaa standardointeja jäsenmaille. Euroopan lentoturvallisuusviraston lisäksi myös jäsenmaat suorittavat valvontaa ja raportoivat näistä Euroopan lentoturvallisuusvirastolle. (Euroopan komissio 2015a) Valvontaa käydään tarkemmin läpi luvussa 3.5.



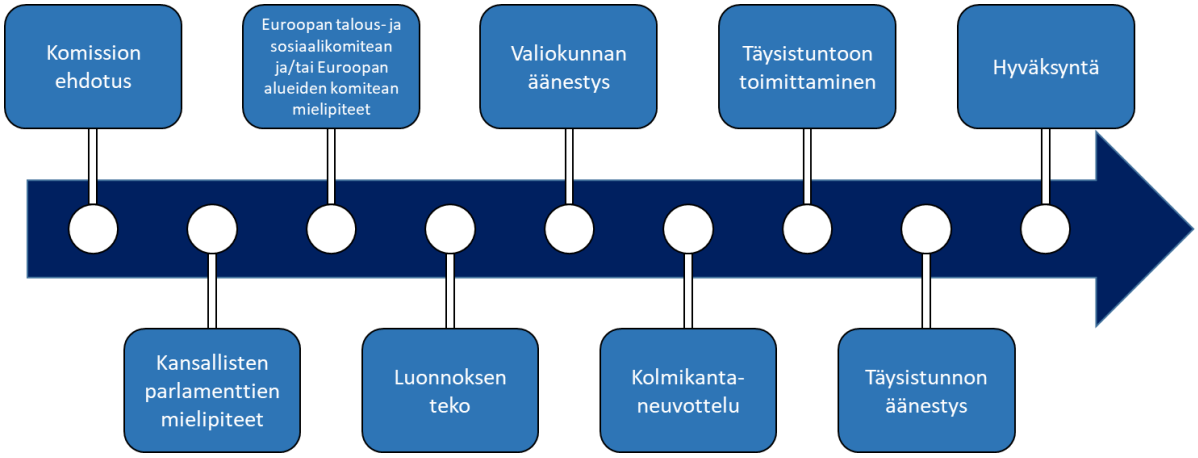
Kuvio 3 Eri toimijoiden välinen vuorovaikutus EU:n turvallisuusjärjestelmässä (mukaillen Euroopan komissio 2015a)

Jäsenmaat ovat ”…vastuussa lentoturvallisuuden varmistamisesta omalla alueellaan ja ilmatilassaan.” Jäsenmaiden tehtävänä ovat myös sertifiointitehtävät, ”…kuten kansallisten organisaatioiden hyväksynnät ja henkilöstön lupakirjat…”. Jäsenmaiden tehtävänä on myös antaa turvallisuussuosituksia Euroopan lentoturvallisuusvirastolle ja maksaa maksua Euroopan lentoturvavirastolle. Maksu on ohjattu viraston toimintaa kohti. Alan sidosryhmät, kuten lentoyhtiöt toimivat Euroopan unionin lainsäädännön alaisena. Lainsäädäntöä valvoo niin kansallinen viranomainen kuin Euroopan lentoturvallisuusvirasto. (Euroopan komissio 2015a)

3.4 Uuden sääntelyn tekeminen prosessina

Kuvio 4 kuvaa Euroopan unionin tavallista lainsäädäntöprosessia, jota myös ilmailulakien säätäminen noudattaa. Kuviossa on kuvattu vuoden 2015 joulukuussa tehdyn säädösehdotuksen prosessi uudesta siviili-ilmailulainsäädännöstä. Menettely alkaa Euroopan komission säädösehdotuksella, jonka se toimittaa Eurooppa-neuvostolle ja Euroopan parlamentille. Sää-

dösehdotus lähetetään samanaikaisesti myös jäsenvaltioiden parlamenteille sekä joissain tapauksissa myös Euroopan alueiden komitealle ja talous- ja sosiaalikomitealle. (Eurooppa-neuvosto 2018a)



Kuvio 4 Euroopan lainsäädäntöprosessin vaiheet (mukaillen Juul 2016)

Ennen parlamentin kannan esittämistä neuvosto voi muodostaa yleisnäkemyksen, jonka avulla parlamentti saa käsityksen neuvoston kannasta säädösehdotukseen. Yleisnäkemys voi nopeuttaa yhteisymmärrystä parlamentin ja neuvoston välillä. Neuvosto, parlamentti ja komissio voivat pitää epävirallisia kolmikantaneuvotteluita säädösehdotuksesta. Neuvotteluiden tarkoituksena on myös nopeampi yhteisymmärryksen löytäminen. Ensimmäisessä käsittelyssä parlamentti voi hyväksyä ehdotuksen sellaisenaan tai tehdä tarkistuksia ehdotukseen. Tämän jälkeen neuvosto voi hyväksyä parlamentin kannan, jolloin säädös annetaan, tai muuttaa parlamentin kantaa, jolloin ehdotus palautetaan parlamentin toiseen käsittelyyn. (Eurooppa-neuvosto 2018b)

Kolmannessa vaiheessa parlamentti voi hyväksyä neuvoston kannan, jolloin säädös annetaan, tai hylätä sen, jolloin säädös ei astu voimaan ja menettely päättyy. Parlamentti voi myös ehdottaa tarkistuksia ja palauttaa säädösehdotuksen neuvostolle toista käsittelyä varten. Mikäli ehdotus palautetaan neuvostolle, neuvosto voi hyväksyä kaikki parlamentin tarkastukset, jolloin säädös annetaan, tai olla hyväksymättä kaikkia tarkistuksia, jolloin kutsutaan koolle sovittelukomitea. (Eurooppa-neuvosto 2018c) Mikäli sovittelukomitea kutsutaan koolle, voi sovittelukomitea sopia yhteisestä tekstistä, joka toimitetaan parlamentille ja neuvostolle kolmatta

käsittelyä varten. Mikäli sopimukseen yhteisestä tekstistä ei päästä, menettely päättyy ja säädöstä ei anneta. (Eurooppa-neuvosto 2018d)

Kolmannessa käsittelyssä Euroopan parlamentti käsittelee sovittelukomitean tekstin. Parlamentti voi hylätä tekstin, jolloin menettely päättyy ja säädös ei tule voimaan, tai hyväksyä tekstin. Mikäli parlamentti hyväksyy tekstin, vaaditaan säädöksen antamiseen vielä neuvoston hyväksyntä. Mikäli neuvosto hylkää sen, menettely päättyy ja ehdotus ei tule voimaan. Mikäli neuvosto hyväksyy tekstin, säädös annetaan voimaan. Mikäli menettely päättyy missään vaiheessa, voidaan uusi menettely aloittaa vain komission uudella ehdotuksella. (Eurooppa-neuvosto 2018e)

3.5 Valvonta ja sääntörikkomukset

Euroopan unioni on kehittänyt ohjelman EU-alueen ulkopuolisten lentokoneiden tarkastamista varten vuonna 1996. Safety Assesment of Foreign Aircraft ohjelman lisäksi unioni vakinaisti vuonna 2006 Safety Assesment of Community Aircraft ohjelman pakolliseksi osaksi jäsenmaiden lainsäädäntöä Euroopan lentoturvallisuusviraston jäsenmaiden lentokoneiden tarkastamista varten. Viraston jäseniä koskeva Euroopan unionin tarkastusohjelma on osittain tarkempi kuin ulkopuolisten maiden lentokoneiden tarkastusohjelma. Tarkastusohjelmat koskevat yli 6000 lentokonetta Euroopan unionin alueella sekä yli 11000 lentokonetta kaikissa osallistuvissa maissa yhteensä. Tarkastusten raportit arkistoidaan Euroopan lentoturvallisuusviraston toimesta. Mahdolliset puutteet tarkastuksissa voivat johtaa toimintalupien peruuttamisiin tai rajoituksiin sekä lentoyhtiön asettamiseen mustalle listalle, joka on ollut voimassa vuodesta 2005 alkaen. Mustaa listaa päivitetään jatkuvasti ja se on julkisesti saatavilla. (Euroopan parlamentti 2018)

Jäsenvaltiot ja niiden kansalliset viranomaiset ovat vastuussa niiden toimien valvonnasta, joiden järjestäminen on jätetty niiden vastuulle. Jäsenvaltiot valvovat näin ollen kansallisia organisaatioita ja maassa toimivia organisaatioita, tekevät tarkastuksia, arviointeja ja auditointeja sekä toimivat sääntöjen noudattamatta jättämisen estämiseksi. Tämän lisäksi jäsenvaltioiden on ”…suoritettava tutkintaa, myös asematasotarkastuksia, ja toteutettava kaikki tarpeelliset

toimenpiteet, ilma-alusten lentokieltoon asettaminen mukaan luettuna.” Euroopan lentoturvallisuusvirasto puolestaan ”…valvoo käytössä olevien ilma-alustyyppien suorituskykyä koko tyyppisuunnitelman mukaisesti valmistetun ilma-aluksen käyttöiän ajan. Tähän liittyen se voi vaatia toimia, jos se havaitsee jonkin turvallisuutta heikentävän seikan.” Tämän lisäksi Euroopan lentoturvallisuusvirasto suorittaa standardointitarkastuksia jäsenvaltioille, joiden avulla se seuraa täytäntöönpanosääntöjen soveltamista. Virasto raportoi tarkastuksistaan Euroopan komissiolle. Virasto voi myös tarkastaa organisaatioita ja ”…huolehtii myös komission puolesta yhteisen eurooppalaisen ilmatilan ilmaliikenteen hallintaverkon toimintojen hallinnoijan valvonnasta.” (Euroopan komissio 2015a)

Euroopan lentoturvallisuusvirasto voi itsenäisesti aloittaa määrätyn menettelyprosessin tilanteissa, joissa sääntelyä tai Euroopan lentoturvallisuusviraston implementointisääntöjä on jätetty noudattamatta. Virasto voi pyytää epäilyn kohteelta tietoja ennen menettelyprosessin aloittamista ja asettaa aikarajan tietojen toimittamiselle. Menettelyprosessissa on erikseen eroteltu vaatimus asettaa ja ilmoittaa aikarajoista prosessin vaiheissa epäillylle. Prosessissa on kuusi vaihetta, jotka ovat ilmoittaminen, tiedustelu, vapaaehtoinen noudattaminen, väitetiedoksianto, suullinen kuuleminen ja raportointi. Mikäli vaiheet eivät tuota tulosta sääntelyn noudattamisen suhteen, raportoi virasto viimeisen prosessin vaiheen mukaisesti Euroopan komissiolle virheellisestä toiminnasta, minkä jälkeen Euroopan komissio tutkii tapauksen ja voi määrätä väärin menettelevälle toimijalle sakon. (Komission täytäntöönpanoasetus 646/2012)

Euroopan komissio valvoo jäsenvaltioiden lainsäädännön soveltamista. Mikäli jäsenvaltion epäillään rikkovan unionin oikeutta, voi komissio ryhtyä toimenpiteisiin. Komissio saa tiedon rikkomuksista Euroopan lentoturvallisuusviraston ilmoituksesta. Komission ensisijainen pyrkimys on ratkaista mahdollinen rike jäsenvaltion kanssa käytävän jäsennellyn vuoropuhelun avulla. Vuoropuhelussa jäsenvaltio voi tuoda komission tietoon oikeudellisia tietoja tai täydentäviä seikkoja asiasta. Mikäli ratkaisua ei löydetä jäsennellyn vuoropuhelun avulla, voi komissio aloittaa virallisen rikkomismenettelyn ja viedä tätä kautta jäsenvaltion lopulta unionin tuomioistuimeen. (Euroopan komissio 2015a)

Komissio voi myös määrätä uhkasakkoja tai sakkoja Euroopan lentoturvallisuusviraston pyynnöstä henkilöille tai yrityksille, joilla on Euroopan lentoturvallisuusviraston myöntämä todis-

tus. Uhkasakkojen ja sakkojen ”…on oltava varoittavia ja sekä tapauksen vakavuuden että asianomaisen todistuksen haltijan taloudellisen kestokyvyn kannalta oikeasuhteisia, kun otetaan huomioon erityisesti turvallisuuden vaarantamisen aste.” Lisäksi komissio voi tarkastaa myönnettyjen todistusten täytäntöönpanosääntöjenmukaisuuden ja vaatia toimivaltaista viranomaista toteuttamaan korjaavia toimenpiteitä mikäli säännöt eivät täyty. Mikäli korjattavat toimenpiteet suoritetaan, päättää komissio todistuksen vastavuoroisesta tunnistamisesta. (Euroopan komissio 2015a)

4 KYBERRISKIT JA NIIDEN VAIKUTUSALUEET SIVIILI-ILMAILUSSA

4.1 Ilmailualan kyberriskien ja kyberturvallisuuden taustaa

Ilmailualalla kyberriskiä käsitellään yhä enemmän kyberturvallisuuden kautta. Kyberturvallisuudessa ovat keskiössä kyberuhat. (ICAO 2018a) Luvussa 2.3 mainitusti kyberriski koostuu omaisuuden arvosta, sitä koskettavasta uhasta ja uhan realisoitumisen vaikutuksen tulosta, minkä vuoksi kyberuhat ovat osa kyberriskiä (Limnéll 2014, 108–109). Aikaisemmin luvussa 2.1 käsitelty kyberriskien globaali olemus ja maantieteellisen sijainnin merkityksen heikentyminen aiheuttaa sen, että riskin toteutuessa esimerkiksi Yhdysvalloissa voi riski vaikuttaa myös Eurooppalaiseen lentoturvallisuuteen, korostaen tasavertaisen ja tasalaatuisen riskienhallinnan tarvetta maailmanlaajuisesti. Jotkin ilmailun järjestelmistä ovat kuitenkin maa- tai aluekohtaisia, minkä vuoksi vain Euroopan ulkopuolella käytössä olevia järjestelmiä ja niihin liittyviä riskejä ei analysoida tarkemmin tässä tutkielmassa.

Luvussa 2.1 käsitelty kyberriski kattaa taloudelliseen menetykseen, keskeytymiseen tai maineen vahingoittumiseen johtavat riskit, jotka aiheutuvat informaatioteknologisesta virheestä. Nämä virheet käsittävät kaikki heikosta järjestelmästä johtuvat operationaaliset virheet, tahalliset ja auktorisoimattomat tietomurrot sekä vahingolliset ja tahattomat tietomurrot. (Institute of Risk Management 2014, 8) Ilmailualalla keskiössä oleva kyberturvallisuus keskittyy pääosin tahallisiin ja auktorisoimattomiin tietomurtoihin sekä vahingollisiin ja tahattomiin tie-

tomurtoihin. Tämän lisäksi alan tutkimukset ovat huomioineet ulkopuolisen mahdolliset vaikutukset kriittisiin järjestelmiin. Siviili-ilmailussa teknologisten laitteiden hajoaminen on ollut alan keskeisenä riskinä jo alan alkuajoista lähtien, minkä vuoksi sitä ei erityisesti käsitellä tässä tutkielmassa. Ilmailualan havaittu käsitys kyberturvallisuudesta on kyberuhkien ja kyberriskien torjunta, sillä ala keskittyy välttämään tai poistamaan kaikki mahdolliset riskit.

Seuraavissa alaluvuissa tuodaan esille aineistosta analysoimalla saadut tulokset, joita on syntetisoitu yhtenäiseen muotoon ja taulukoitu esiintymiskertojen perusteella.

4.2 Systemaattinen kirjallisuuskatsaus kyberriskien vaikutuksesta kaupalliseen siviili-ilmailuun

Toteutuneita kyberriskejä ja niiden vaikutuksia kyberturvallisuudelle käytiin nopeasti läpi luvussa 1.1, jossa esiteltiin tutkimuksen taustaa. Kirjallisuuskatsauksella halutaan nähdä tutkimusten johtopäätöksiä siitä, mitä kyberriskejä tai niitä muodostavia uhkia ja haavoittuvuuksia voidaan tunnistaa sekä selvittää miten ne vaikuttavat siviili-ilmailun kyberturvallisuuteen. Haassin ym. (2016, 39) mukaan:

> *”Seuraavan kymmenen vuoden aikana miehitettyjen ja miehittämättömien lentokoneiden sekä järjestelmien ja uusien teknologisten ominaisuuksien määrä tulee kasvamaan. Kyberteknologia, mukaan lukien ohjelmistot, tietokoneverkot ja informaatioteknologia ovat kriittisessä ja perustavanlaatuisessa asemassa, jotta tulevaisuuden tarpeet voidaan huomioida ilmailun ekosysteemin osalta. – Suurista hyödyistä huolimatta kyberteknologia altistaa ilmailun vaarallisten ja kalliiden uhkien maailmalle. Uhkat itsessään eivät ole uusia alalle ja ala on kasvanut toimimaan luonnon ja ihmiskunnan fyysisten vastoinkäymisten keskellä. Mutta yhden vuosisadan lentotoiminta ei turvallisuuden ja tehokkuuden riskienhallinnan kokonaisvaltaiseksi hallitsemiseksi. Uhkat kyberturvallisuudelle asettavat merkittävän haasteen – hyökkäyksen arvaamattomuus tekee riskistä vaikeasti ymmärrettävän. Tämän lisäksi mahdollisuudet hyökkäyksille lisääntyvät uusien palveluiden ja järjestelmien kehityksen myötä.” (Haass ym. 2016, 39)*

Myös Stander & Ophoff (2016, 23–24) mainitsevat, että erityisesti yhteen liitettyjen tietojärjestelmien yleistyminen tulee lisäämään ilmailualan haavoittuvuutta tulevaisuudessa. Strohmeier ym. (2017) huomauttavat, ettei mikään lennonjohdon langattomista viestintälaitteista ole käsitteellisestä näkökulmasta katsottuna turvallinen, sillä turvallisuus ei koskaan ollut osana niiden suunnittelua. Strohmeierin ym. (2017) mukaan akateeminen yhteisö ja hakkerointiyhteisö ovat lähiaikoina demonstroineet miten järjestelmien haavoittuvuuksia voidaan käyttää hyväksi hyökkäyksissä, mutta kaikkia näitä demonstraatioita ei kuitenkaan ole huomioitu ilmailun toimialalla. Kessler & Craiger (2018, 34) toteavat kyberhyökkäysten uhkaavan koko ilmailualan olemassaoloa, mikäli niihin ei kiinnitetä huomioita.

Taulukko 4 Kyberturvallisuuteen vaikuttavat uhkat ja niiden alkuperät

Vaikutuskohde	**Uhka**	**Esiintymä**
ADS-B järjestelmä	Etähyökkäys, häiriö, ihmisvirhe, koulutustoiminta	T1, T2, T3, T4
GPS-paikannusjärjestelmä	Etähyökkäys, häiriö, haittaohjelmat	T1, T2, T3, T4
ACARS-järjestelmä	Etähyökkäys	T2, T3, T4
Henkilökunta	Tahallinen virhe, lähihyökkäys, haittaohjelmat	T1, T2
Lentokoneiden viihdejärjestelmät	Lähihyökkäys	T1, T2
Lentohenkilökunnan omat laitteet	Haittaohjelmat	T1, T2
Miehittämättömät ilma-alukset	Etähyökkäys, käyttö toiseen hyökkäykseen	T1, T3
TIS-B ja FIS-B järjestelmät	Etähyökkäys	T2, T4
Wi-Fi-verkot	Etähyökkäys, lähihyökkäys	T1
Verkon yhteyskäytännöt	Etähyökkäys	T1
Avoimen lähdekoodin järjestelmät	Etähyökkäys	T1
Virtualisointi	Etähyökkäys	T1
Pilvipalvelut	Etähyökkäys	T1
Tietokoneen toimintavika	Sää tai luonnonkatastrofi	T1
Lentokoneen lennonhallintajärjestelmät	Etähyökkäys yhteysjärjestelmien kautta	T2
Ilmailualan tietokoneiden järjestelmät	Haittaohjelmat	T3
Toimitusketjut	Etähyökkäys	T3
Asioiden internet	Etähyökkäys	T3
Lennonjohdon ääniviestintäjärjestelmä	Etähyökkäys	T4
Tutkajärjestelmät	Etähyökkäys	T4
Törmäysvaroitusjärjestelmä	Etähyökkäys	T4

Haavoittuvuudet ja niiden mahdollistamat hyökkäykset ovat siis tutkimusten mukaan vahvasti kyberturvallisuuden keskiössä, mutta mihin hyökkäyksiä voidaan kohdistaa ja miten hyökkäykset vaikuttavat kyberturvallisuuteen?

Taulukossa 4 on esitelty koostettuna kyberturvallisuuteen vaikuttavien uhkien ja niiden vaikutuskohteiden luettelo. Taulukon tulokset on jaoteltu kirjallisuuskatsausaineiston esiintymiskertojen perusteella. Koosteen perusteella voidaan huomata, että ADS-B-, GPS- ja ACARS-järjestelmät olivat tutkimuksissa eniten esiintyneet vaikutuskohteet. Koosteesta voidaan myös huomata etähyökkäysten olevan pääasiallinen uhkan lähde. Koosteesta kahdeksan vaikutuskohdetta esiintyvät kahdessa tai useammassa kuin kahdessa valituista neljästä tutkimuksesta. TIS-B ja FIS-B järjestelmät ovat Yhdysvaltain ilmailuviraston järjestelmiä ja ne rajataan kansallisen Euroopan ulkopuolisen vaikutuksen vuoksi pois tarkemmasta analyysistä. (Stander & Ophoff 2016, 25) Kirjallisuuskatsauksella halutaan tiivistää ja analysoida tutkimusten yhtymäkohtia ja vertailla mahdollisia eroavaisuuksia mainituista uhkien vaikutuksista. Tämän vuoksi havaintoja, jotka esiintyivät vain yhdessä kirjallisuuskatsauksen tutkimuksista, ei analysoida tarkemmin.

4.2.1 ADS-B- ja GPS-järjestelmä

Ilmailualan kyberuhkien vaikutuskohteiden synteesi nosti aineistosta esiin erityisesti ADS-B- ja GPS-järjestelmien uhkia ja haavoittuvuuksia. Järjestelmät mainittiin jokaisessa kirjallisuuskatsaukseen valituista aineistoista. Järjestelmiä käsitellään yhdessä, sillä ne ovat kietoutuneina toisiinsa. Standerin & Ophoffin (2016, 25) mukaan:

> *”Automatic-Dependent Surveillance-Broadcast (ADS-B) on satelliittipohjainen järjestelmä, joka toimii seuraajana tutkalle ilmailussa. Se perustuu konseptiin, jossa jokainen osallinen saa oman sijaintinsa ja nopeutensa kyydissä olevasta GPS-järjestelmästä ja lähettää säännöllisesti kyseisiä tietoja viestillä ADS-B Out-alijärjestelmän kautta. Nämä tiedot vastaanotetaan lentoliikenteen valvonta-osapuolien sekä muiden lentokoneiden toimesta, joissa on ADS-B In-alajärjestelmä.” (Stander & Ophoff 2016, 25)*

Strohmeier ym. (2017) mainitsevat järjestelmän käyttöönoton tulevan pakolliseksi vuoteen 2020 mennessä niin Euroopan kuin Yhdysvaltojen ilmatiloissa, millä pyritään parantamaan paikannustarkkuutta ja vähentämään järjestelmäkustannuksia.

Haass ym. (2016, 42) kertovat GPS-järjestelmä Global Navigation Satellite Systemin tuottavan kriittistä navigaatiotietoa ADS-B-järjestelmän kautta ja luokittelevat GNSS-järjestelmän heikkoihin radiotaajuusjärjestelmiin, joiden kautta voi olla mahdollista suorittaa haittaohjelmahyökkäyksiä yhteydessä oleviin järjestelmiin. Strohmeierin ym. (2017) mukaan ADS-B järjestelmä kärsii samoista passiivisista ja aktiivisista hyökkäyksistä kuin sitä edeltävät järjestelmät. Haass ym. (2016, 41) määrittelevät passiivisen hyökkäyksen olevan hyökkäys, jossa hyökkääjä vain kuuntelee ja tarkkailee hyökkäyksen kohdetta. Aktiivisella hyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkääjä lähettää signaaleita tai dataa ja vastaanottaa niihin vastauksia. Hyökkäys voi myös olla passiivis-aktiivinen, jossa käytetään molempia hyökkäystapoja. (Haass ym. 2016, 41)

Strohmeierin ym. (2017) mukaan ADS-B-järjestelmän viestejä voidaan estää ruuhkauttamalla palvelin, joka aiheuttaisi ruuhkautuksesta kärsivän lentokoneen katoamisen järjestelmän kanavalta. Järjestelmään syötetyillä väärennetyillä tiedoilla voidaan luoda olemattomia lentokoneita, jotka näkyvät järjestelmässä. Väärennettyjä lentokoneita ei ole mahdollista tunnistaa oikeista lentokoneista järjestelmän yhteystasolla. Järjestelmän lähettämiä, lennonjohdolle näkyviä sijaintitietoja voidaan myös väärentää estämällä lentokoneen signaali ja lähettämällä muutettua signaalia estetyn signaalin tilalle. Tämä aiheuttaa ristiriitaisia tietoja oikean sijainnin ja lennonjohdon näkemän sijainnin välillä. (Strohmeier 2017)

Kesslerin & Craigerin (2018, 14) mukaan ADS-B-järjestelmästä puuttuu salaus- ja turvallisuusominaisuuksia, jotka voivat altistaa järjestelmän kyberhyökkäysten työkaluiksi. Heidän mukaansa ADS-B-järjestelmän tietoja on julkisesti saatavilla, sillä niitä käytetään usean verkkosivuston toimesta lentojen seuraamiseen. Strohmeier ym. (2017) ovat myös sitä mieltä, että järjestelmän lähettämät sijaintitiedot avaavat uusia haavoittuvuusreittejä. Heidän mukaansa tietojen hyväksikäyttämiseen tarvitaan vain niin kutsuttua helposti hankittavissa olevaa tietoteknologista vakiokalustoa. Stander & Ophoff (2016, 25) ovat samaa mieltä siitä, ettei ADS-B-järjestelmän viestien peukalointi vaadi hienostuneita laitteita. Suuren luokan signaalinestohyökkäyksiä he pitävät kuitenkin vaikeina toteuttaa. Tämän lisäksi he kertovat järjestelmän

viestien peukaloinnin olevan kohtuullisen helppoa, mutta viestien peukaloinnin tunnistamisen olevan vaikeaa. He mainitsevat myös, ettei järjestelmän protokolla vaadi tunnistautumista, joka heikentää järjestelmän turvallisuutta. (Stander & Ophoff 2016, 25)

Kessler & Craiger (2018, 13) esittelevät ADS-B järjestelmän uhkia Purtonin, Husseinin & Alamin (2010) tutkimuksen taulukon kautta. Taulukko avataan lähteenä käytetyn Purtonin ym. (2010) tutkimuksen avulla, sillä Kesslerin & Craigerin (2018) julkaisu ei avaa taulukkoa esityksen puitteissa.

Taulukko 5 Kesslerin & Craigerin (2018) esittämät ADS-B-järjestelmän uhat (mukaillen Purton ym. 2010)

Uhka	Tyyppi	Todennäköisyys	Vakavuus	Vaikutus
GPS: Palvelunesto	Tahallinen	Matala	2	Saatavuus
GPS: Toimintavirhe	Häiriö	Keskitaso	2	Eheys
ADS-B: Sammuttaminen	Tahallinen	Matala	1	Saatavuus
ADS-B: Toimintavirhe	Häiriö	Keskitaso	3	Eheys
Tietokanava: Häirintä	Tahallinen	Keskitaso	3	Saatavuus
Tietokanava: Viivästynyt uudelleenlähetys	Tahallinen	Matala	4	Saatavuus
Tietokanava: Väärennetyt signaalit	Tahallinen	Keskitaso	2	Eheys
Tietokanava: Liiallinen bittivirhesuhde	Häiriö	Korkea	2	Saatavuus
Maa-asema: Tahallinen vahingoittaminen	Tahallinen	Matala	2	Saatavuus
Maa-asema: Datan manipulointi	Tahallinen	Matala	2	Eheys
Maa-asema: Koulutusviive	Ihmisvirhe	Keskitaso	3	Saatavuus ja eheys

Taulukossa 5 luokitellaan ADS-B-järjestelmän uhat tyypin, todennäköisyyden ja vakavuuden mukaan. Vakavuusluokitteluna taulukossa on käytetty EUROCAEn, eli Euroopan siviili-ilmailulaitteisto-organisaation (European Organisation for Civil Aviation Equipment) tekemää vaaraluokittelua, joka luokittelee uhat ja vaarat numeroittain asteikolla yhdestä viiteen, yhden ollessa vakavin ja viiden ollessa lievin vakavuusaste. (Purton ym. 2010, 7)

Asteikon vaaraluokalla yksi tarkoitetaan tapahtumia, jotka voivat toteutuessaan aiheuttaa lentokoneen kontrollin totaalisen menettämisen, putoamisen, törmäyksen toiseen lentokoneeseen ilmatilassa tai kontrolloidun laskeutumisen maastoon. Vaaraluokan kaksi omaavat tapahtumat voivat aiheuttaa erittäin merkittävän turvallisuusmarginaalien vähentymisen, erittäin merkittävän lentokoneen toiminnan häiriön tai yhteyden menettämisen lennonjohtoon merkittävän pitkäksi ajaksi. Kolmannen vaaraluokan tapahtumat voivat aiheuttaa huomattavan

turvallisuusmarginaalien ja lentokoneen toiminnan vähentymisen sekä vaikuttaa huomattavasti yhteyteen lennonjohdon kanssa. Neljännen vaaraluokan tapahtumat voivat vähentää turvallisuusmarginaaleja, lentokoneen toimivuutta ja yhteyttä lennonjohtoon vähäisessä määrin, kun taas viidennen luokan tapahtumat eivät vaikuta turvallisuusmarginaaleihin tai lentokoneen toimivuuteen. (Purton ym. 2010, 7)

Taulukossa 5 ADS-B järjestelmäuhkista kaksi pohjautuvat GPS-järjestelmään. Uhkat ovat palvelunesto ja toimintavirhe. ADS-B järjestelmä käyttää lentokoneen omaa GPS-järjestelmää toimiakseen. Kumpikin näistä tapahtumista ovat vaaraluokassa kaksi, aiheuttaen tapahtuessaan erittäin merkittäviä turvallisuusvaikutuksia. Palvelunesto on luokiteltu tahalliseksi matalan todennäköisyyden tapahtumaksi, sillä GPS-järjestelmä toimii laajalla signaalitaajuusskaalalla, minkä vuoksi järjestelmän palvelunesto maasta käsin vaatisi erityisen tehokkaan välineistön. Strohmeierin ym. (2017) mukaan GPS-signaalit ovat kuitenkin erittäin heikkoja, minkä vuoksi niiden palvelunestoon ei vaadita erityisen tehokasta häirintäsignaalia.

Purtonin ym. (2010, 6) mukaan GPS-järjestelmän palvelunesto voi tapahtua myös lentokoneen yläpuolelta, mutta vaatisi toimiakseen sotilaslentokoneen tai vastaavan välineistön. Toimintavirhe on luokiteltu häiriöksi ja todennäköisyydeltään keskiluokkaan, sillä satelliittien signaalivirheitä tapahtuu ajoittain heikentäen järjestelmän paikannuksen tarkkuutta. Järjestelmät ovat kuitenkin kykeneväisiä erottelemaan huonot signaalit ja jättämään ne pois käytöstä mikäli se parantaa järjestelmän tarkkuutta, heikentäen tapahtuman todennäköisyyttä. (Purton ym. 2010, 7)

Strohmeierin ym. (2017) mukaan signaalin heikkouden vuoksi palvelunestohyökkäys GPS-järjestelmään on alalla hyvin tunnettu heikkous ja hyökkäyksen järjestäminen luokiteltu helpoksi. Heidän mukaansa myös GPS-signaalin väärentäminen on mahdollista ja voi aiheuttaa vakavia tapahtumia. Signaalin väärentämistä ei huomioida Purtonin ym. (2010) tutkimuksessa. Stander & Ophoff (2016, 25) mainitsevat, että maasta käsin väärennetty signaali näkyisi myös läheisille vastaanottajille, joka tekee hyökkäyksestä epätodennäköisen.

Strohmeierin ym. (2017) kyselytutkimus osoitti myös, että vain noin 30 % vastanneista tiesivät GPS-järjestelmän turvallisuuspuutteista ja noin 50 % uskoi järjestelmän sisältävän sisäänrakennettua turvallisuusteknologiaa. Löydökset ovat heidän mukaansa huolestuttavia. GPS-jär-

jestelmän lisäksi lentämisessä käytetään heidän mukaansa useita muita navigaatiojärjestelmiä, minkä vuoksi hyökkäys yhteen järjestelmään ei aiheuttaisi kriittistä vaikutusta. Yhteen järjestelmään hyökkäys aiheuttaisi kuitenkin komplikaatioita, jotka nostavat virheellisen toiminnan riskiä. (Strohmeier ym. 2017)

Taulukon 5 uhkista kolmas on ADS-B järjestelmän tahallinen sammuttaminen, joka on luokiteltu vakavimpaan vakavuusluokkaan taulukossa. Mikäli järjestelmä sammutettaisiin tahallisesti, aiheuttaisi se lennon vastaamattomuuden lennonjohdolle, jolloin lennonjohto joutuisi seuraamaan lentoa vain tutkan ja lentosuunnitelmien perusteella. Tapahtuman todennäköisyys on luokiteltu matalaksi, sillä se vaatii tahallisia tietoisia toimia lentokoneen ohjaamosta käsin. Julkisesti uhka on usein vastaanotettu todennäköisempänä, sillä vastaavanlainen tahallinen paikannusjärjestelmän sammutus tapahtui aiemmalla järjestelmällä vaikeuttaen merkittävästi lentokoneiden paikannusta vuoden 2001 syyskuussa tapahtuneessa terroristi-iskussa. (Purton ym. 2010, 7) Muut tutkimukset eivät ottaneet kantaa tahalliseen sammuttamiseen.

Taulukossa 5 on neljänneksi uhaksi merkitty häiriöstä johtuva toimintavirhe ADS-B järjestelmälle. Toimintavirheen pääasiallisiksi syiksi on tunnistettu virheelliset syöttötiedot järjestelmään sekä lähettimen toimintahäiriö. Virheellistä syöttötietoa ei välttämättä voida tunnistaa, mutta lähettimen toimintahäiriön tunnistaminen puolestaan on todennäköistä, minkä vuoksi tapahtuman todennäköisyys on keskitasoa. ADS-B järjestelmän toimintahäiriö on luokiteltu kolmanteen vakavuusluokkaan, aiheuttaen toteutuessaan merkittävän turvallisuusvaikutuksen. (Purton ym. 2010, 7) Strohmeier ym. (2017) mainitsevat viestien peukaloinnin, eli tahallisen virheellisen syötön olevan mahdollista, mutta vaikeaa. He eivät kuitenkaan ota kantaa tapahtuman vaikutuksiin.

Taulukon 5 listaamilla tietokanavauhkilla tarkoitetaan uhkia, jotka vaikuttavat lentokoneen, maa-aseman ja lennonjohdon välillä olevaan tietokanavaan. Näitä tietokanavan uhkia ovat häirintä, viivästynyt uudelleenlähetys, väärennetyt signaalit ja liiallinen bittivirhesuhde. Tietokanava on Purtonin ym. (2010, 8) mukaan herkin osa-alue kriittisten uhkien osalta. Häirinnällä tarkoitetaan maasta käsin tapahtuvaa tahallista signaalin ruuhkauttamista, mikä estää taajuudella tapahtuvan viestinnän. Signaalin häirintä on huomattavasti helpompaa maasta kuin ilmasta käsin, sillä valitulla taajuudella on luonnostaan paljon signaaleja useiden lentokoneiden toimesta. Uhka on luokiteltu todennäköisyydeltään keskitasolle ja vakavuusaste on luokiteltu

kolmanteen luokkaan. (Purton ym. 2010, 8) Stander & Ophoff (2016, 25) sanovat laajaskaalaisen signaalin häirinnän olevan vaikeaa, mutta eivät ota kantaa vaikutuksiin.

Viivästyneellä uudelleenlähetyksellä tarkoitetaan tahallista signaalin viivästyttämistä kolmannen osapuolen kautta. Merkittävä viivästyminen voi aiheuttaa lentokoneen havaitun aseman tärinänomaista liikettä kartalla. Pahimmassa tapauksessa maa-aseman signaaleja ei voida käyttää aiheuttaen käytännössä saman asian mitä häirintä aiheuttaa. Uudelleenlähetyksen viivästymisen todennäköisyys on taulukossa 5 luokiteltu matalaksi ja sen vakavuus on asetettu matalammaksi kuin häirinnällä, asettaen sen vakavuusluokkaan neljä. (Purton ym. 2010, 8) Strohmeier ym. (2017) mainitsevat signaalin viivästyttämisen estämisen olevan kallista toteuttaa, minkä vuoksi viivästyttämisen estäminen on käytännössä mahdotonta.

Tahalliset väärennetyt signaalit ovat merkittävä uhka, sillä niillä voidaan tahallisesti aiheuttaa erittäin merkittäviä turvallisuusvaikutuksia keskitason todennäköisyydellä. Merkittävän operatiivista toimintaa häiritsevän väärennetyistä ADS-B signaaleista tekee se, että niillä voidaan huijata lentokoneita ja lennonjohtoa havaitsemaan järjestelmässä väärennettyjä lentokoneita ilmatilassa. Väärennetyt signaalit voivat aiheuttaa törmäysvaroituksia ja suurta hämmennystä. Yhdysvalloissa kansallinen lentoturvallisuusvirasto on luonut tämän varalle identiteettitarkastusohjelman, jolla pyritään estämään väärennettyjen lentokoneiden vaikutusta lentotoimintaan. Tätä varotointa voidaan myös manipuloida, mutta se vaikeuttaa väärennetyillä signaaleilla suuren hämmennyksen ja vaaratilanteiden luomista. (Purton ym. 2010, 8) Strohmeier ym. (2017, 25) mainitsevat myös väärennettyjen signaalien mahdollisuuden, mutta eivät ota kantaa uhkan vakavuuteen.

Tietokanavan liiallinen bittivirhesuhde on järjestelmän häiriö, joka voi aiheuttaa järjestelmän kantavuuden heikentymistä esimerkiksi säästä johtuen. Bittivirhesuhteen lisäksi taulukossa 5 on liitetty samaan luokkaan monitievastaanotto, jolla tarkoitetaan lähetetyn signaalin eriaikaista vastaanottoa kohteessa. Tämä voi aiheutua esimerkiksi signaalin heijastuessa rakennuksista tai maastosta, kuten vuorista. Häiriö voi aiheuttaa erittäin merkittäviä turvallisuusvaikutuksia korkealla todennäköisyydellä. (Purton ym. 2010, 8–9) Muut tutkimukset eivät huomioi bittivirhesuhdetta.

Maa-asemien uhkina ovat taulukossa 5 tunnistetut tahallinen vahingoittaminen, datan manipulointi ja koulutusviive. Maa-asemat voidaan jakaa maa-asemavastaanottimiin ja lennonjohdon näyttöjärjestelmiin. Maa-asemien osalta tahallinen vandalisointi olisi kohtuullisen helppoa ja poistaisi käytöstä maa-aseman kokonaisuudessaan. Vandalisoinnilla voitaisiin saavuttaa erittäin merkittävä turvallisuusvaikutus, mutta vandalisoinnin todennäköisyys on luokiteltu silti matalaksi, sillä niiden vandalisointi on historiallisesti ollut epätodennäköistä. Datan manipuloinnilla tarkoitetaan maa-aseman tietomurron kautta tapahtuvaa tiedon tahallista muuntamista. Murto voisi aiheuttaa suurimman vaarallisuusluokan tasoisia turvallisuusvaikutuksia, mutta vaatisi merkittävän korkeatasoista laitteistoa ja osaamista, minkä vuoksi tapahtuman todennäköisyys on luokiteltu matalaksi. (Purton ym. 2010, 9) Muut tutkimukset eivät myöskään ota kantaa tahalliseen maa-aseman vahingoittamiseen.

Koulutusviiveellä tarkoitetaan uuden teknologian ja sen vaatiman koulutuksen aiheuttamia häiriötilanteita, joissa henkilöstö ei puutteellisen taidon tai tiedon johdosta osaa toimia tai reagoida oikein. ADS-B järjestelmän signaaleita näyttävä järjestelmä lennonjohdossa on monimutkainen, mikä voi aiheuttaa epäselvyyksiä ja virheitä. Koulutusviive onkin huomioitava erityisesti yhteydessä muihin ongelmiin, jolloin ongelmanratkaisu ja järjestelmätieto nousevat keskiöön. Yhteytensä ansiosta tapahtuman todennäköisyys on määritelty keskitasolle ja vakavuus itsessään on asetettu kolmannelle tasolle. Tapahtuma voi siis aiheuttaa toteutuessaan huomattavia turvallisuusvaikutuksia. (Purton ym. 2010, 9) Myöskään koulutusviivettä ei huomioida muissa tutkimuksissa.

Strohmeierin ym. (2017) mukaan ADS-B-järjestelmän ongelmat ovat huolestuttavia, sillä järjestelmän on tarkoitus toimia pääasiallisena pitkän aikavälin työkaluna lentoliikenteen valvonnassa. Heidän toteuttamansa kyselytutkimuksen mukaan ADS-B- ja GPS-järjestelmien arvioitiin olevan todennäköisin kohde hyökkäykselle. Kuitenkin vain 20 % heidän teettämään kyselyyn osallistuneista lentäjistä ja lennonvalvojista olivat tietoisia järjestelmän puutteista.

Syntetisoidun aineiston mukaan tutkimukset tunnistivat monia järjestelmiä kohtaavia kyberriskejä, mutta eivät pitäneet tahallisten hyökkäysten todennäköisyyttä ADS-B- tai GPS-järjestelmiin korkeana. Haassin ym. (2016, 42) mukaan tietoisuuden puute, järjestelmien ongelmat

ja muut vaikuttavat olosuhteet, kuten sää, voivat tehdä ongelmatilanteista vaikeasti käsiteltäviä. Tutkimusten synteesistä voidaan havainnoida esimerkiksi GPS-järjestelmän häirinnän osalta eriäviä mielipiteitä.

Useiden uhkien kohdalla uhkaa oli käsitelty vain yhdessä tutkimuksista. Näin ollen voidaan havainnoida, että riskitietoisuus ja uhkien tietoisuus ei ole vielä vakiintunut samalle tasolle. Voidaan siis havainnoida, että tällä hetkellä ADS-B järjestelmän osalta lähi- ja etähyökkäysten vaikutusten kyberturvallisuuteen arvioidaan pysyvän maltillisina. Toimintavirheistä ei voida vetää yleistäviä johtopäätöksiä, sillä niitä käsiteltiin vain Purtonin ym. (2010) toimesta.

4.2.2 ACARS-järjestelmä

ACARS-järjestelmä oli seuraavaksi eniten tutkimuksissa esiintynyt järjestelmä. Standerin & Ophoffin (2016, 25) mukaan:

> *"Aircraft Communications Addressing and Reporting System (ACARS) on useimpien lentoyhtiöiden käyttämä maan ja ilman väliseen tietokommunikointiin tarkoitettu infrastruktuuri, jonka avulla kommunikoidaan lentoliikenteen valvojien, kansallisten ilmailuviranomaisten ja yhtiöiden omien toimintakeskusten kanssa." (Stander & Ophoff 2016, 25)*

Järjestelmä käyttää satelliitti- ja korkeataajuusviestintää. Viestinnän avulla lähetetään esimerkiksi lentoonlähtö-, laskeutumis- ja säätietoja. Tämän lisäksi järjestelmän kautta kommunikoidaan muun muassa navigaatiotietoja, lentokoneen sijaintiraportteja, lähtölupia ja kiitoratojen olosuhteita. (Stander & Ophoff 2016, 25) Strohmeier ym. (2017) lisäävät järjestelmän lähettävän myös turvallisuudelle kriittistä tietoa muun muassa lentokoneen painon, polttoaineen määrän, moottoritietojen, matkustajien, aikataulujen ja lentosuunnitelmien päivitysten osalta.

Standerin & Ophoffin (2016, 25) mukaan järjestelmän tiedot ovat salaamattomia ja helposti tulkittavissa, mikä voidaan havaita useiden lentokoneiden tietoja välittävien sivustojen, kuten FlightRadar24:n kautta. Heidän mukaansa tietoja voidaan myös lähettää järjestelmään, mutta sen vaikutuksia tutkimuksessa ei arvioida. Strohmeier ym. (2017) nostavat esiin järjestelmän

salaamattomuuden ja mainitsevat tietojen saannin helpottuneen internetin tulkintapalveluiden vuoksi. Kessler & Craiger (2018, 14) mainitsevat myös järjestelmän tietojen salaamattomuuden ja toteavat järjestelmän lentosuunnitelmatietojen olevan väärennettävissä. He kertovat myös, että ADS-B-järjestelmän tavoin tietojen salaamattomuus ja helppo saatavuus verkkosivustojen kautta voivat helpottaa hyökkäysten tekemistä, sillä järjestelmän kautta saadaan tieto lentokoneessa käytettävästä lennonhallintajärjestelmästä (Kessler & Craiger 2018, 14).

Kesslerin & Craigerin (2018, 11, 14) mukaan ACARS-järjestelmään voidaan hyökätä etäältä käsin ja sen tietoja voidaan väärentää. Heidän mukaansa hyökkäystä ACARS-järjestelmään epäiltiin pääsyyksi vuonna 2015 Puolassa tapahtuneeseen välikohtaukseen, jonka vuoksi kymmenen lentokonetta jouduttiin joko ohjaamaan takaisin maahan tai niiden käskettiin olla lähtemättä kentältä. Strohmeier ym. (2017) kertovat myös, että järjestelmän lennonjohtoviestien väärentäminen on mahdollista. He kuitenkin mainitsevat, että järjestelmän heikkoa salausta ja viestien tulkinnan helppoutta on koitettu estää standardin mukaisella lisäohjelmalla, joka parantaa järjestelmän salaustasoa. Heidän mukaansa lisäsalausta ei kuitenkaan ole otettu laajalti käyttöön ja esimerkiksi Ryanair on luopunut kokonaisuudessaan ACARS-järjestelmän käytöstä. He mainitsevat kuitenkin, että järjestelmän turvallisuutta parantaa lentoyhtiöiden omien lyhenteiden käyttö, jotka vaikeuttavat viestin tulkintaa. (Strohmeier ym. 2017)

Kessler & Craiger (2018, 11) kertovat joidenkin asiantuntijoiden olevan sitä mieltä, ettei järjestelmään syötettyjä väärennettyjä tietoja voida pitää turvallisuusongelmana, sillä ne aiheuttavat vain hämmennystä, jonka lentäjä huomaa ja korjaa näin ollen tilanteen. Kesslerin & Craigerin (2018, 11) mukaan eri lentokonejärjestelmät näyttävät ACARS-järjestelmän tiedot eri tavalla, mikä voi pahentaa ongelmaa joissakin lentokonetyypeissä. Strohmeier ym. (2017) muistuttavat, että voidaan helposti kuvitella vaikutuksia, mikäli matkustajalistoja sekä henkilöstö- ja moottoritietoja lähetetään selkeällä tekstillä järjestelmän kautta.

Vaikutuksilla viitataan siihen, että tiedot ovat tällöin helposti saatavissa ja aiheuttavat näin ollen tietojen vuotamisen. Voidaan myös havainnoida, että hämmennystä aiheuttavia tilanteita voitaisiin pitää turvallisuutta alentavana tilana, sillä aiemmin ADS-B järjestelmän osalta Haassin ym. (2016, 42) mainitsema tietoisuuden puute, järjestelmien ongelmat ja muut vai-

kuttavat olosuhteet, kuten sää, voivat tehdä ongelmatilanteista vaikeasti käsiteltäviä. Lisähämmennys voi siis kertaantua muiden vaikutusten kanssa ja aiheuttaa näin ollen turvallisuusvaikutuksia. Etähyökkäysten voidaan jo havainnoida vaikuttaneen konkreettisesti kyberturvallisuuteen, mistä esimerkkinä toimi aiemmin esiin nostettu Puolan LOT-lentoyhtiön tapahtuma. Kyberturvallisuuden heikentymisen mahdollisuus on myös selkeästi olemassa hyökkäysten osalta, sillä vaikka lentäjä huomaisi ja korjaisi tilanteen, alentaa se silti turvallisuutta ainakin hetkellisesti. Mikäli järjestelmän kautta lähetettäisiin huolimattomasti selkeäkielisiä viestejä, joista voitaisiin varastaa matkustaja- ja henkilöstötietoja, voisi luottamuksen alentuminen olla myös merkittävä uhka kyberturvallisuudelle.

4.2.3 Muut vaikutuskohteet

Henkilökunnasta vaikutuskohteena puhutaan tutkimuksissa vain lyhyesti. Haassin ym. (2016, 40) mukaan sisäpiirin uhat tulee ottaa huomioon kyberturvallisuuteen vaikuttavien kyberriskien tarkastelussa. Haass ym. (2016, 40) mainitsevat, että:

> *”Lisäksi lähiaikoina tapahtunut Germanwingsin lento, jossa lentäjä väitetysti ohjasi koneen tahalliseen törmäykseen, viittaa sisäpiirin uhkien mahdollisuuteen ja tarpeeseen hallinnoida niitä ihmisiä paremmin, joilla on oikeutettu pääsy järjestelmään.” (Haass ym. 2016, 40)*

Tämän lisäksi Haass ym. (2016, 40) mainitsevat, että ”…kyberhyökkäyksestä aiheutuneet ongelmat, kuten väärennettyjen lentokoneiden näkyminen tutkajärjestelmässä, voivat myötävaikuttaa turvattomiin päätöksiin ja perusteettomiin suorituskyvyn menetyksiin.” Voidaan siis havainnoida, että uhkien kerroinvaikutus voi mahdollisesti tehdä uhkasta arvioitua suuremman.

Stander & Ophoff (2016, 26) tuovat esiin, ettei lentäjien suorituksista kyberhyökkäysten aiheuttamien poikkeustilanteiden aikana ole tehty tutkimusta. He esittävät kuitenkin kysymyksen, joka kysyy: ”Epäilisikö hyvin koulutettu lentäjä edes, ettei hälytystila ole oikea eikä näin ollen reagoisi siihen mitenkään?” Kysymys on ajatuksia herättävä, mutta ei suoranaisesti vastaa lentäjien mahdollisiin reaktioihin. Kysymyksen lisäksi Stander & Ophoff (2016, 26) mainit-

sevat myös, ettei huoltohenkilökunnan mahdollisuutta päästä käsiksi laitteisiin tai kulunvalvonnan vaarantumista voida ohittaa uhkia tarkastellessa. Tutkimus ei kuitenkaan arvioi uhkia tai esitä niistä lisätietoja.

Lentohenkilökunnan omilla laitteilla viitataan Haassin ym. (2016, 42) tutkimuksessa elektroniseen lentäjänlaukkuun, joka sisältää ohjaamoon vietävän lentopakkauksen. Tämä sisältää esimerkiksi elektronisia karttoja. Tutkimuksessa mainitaan elektroninen lentäjänlaukku, mutta ei erotella sen mahdollisia uhkia. Stander & Ophoff (2016, 26) mainitsevat, että joihinkin laitteisiin olisi helppo ladata haittaohjelmia, joiden avulla voitaisiin välttää tarve päästä käsiksi järjestelmiin verkkojen kautta. Tutkimus ei kuitenkaan erottele laitteita, joiden avulla järjestelmiin voitaisiin välittää haittaohjelmia tai joiden kautta niihin voitaisiin päästä käsiksi.

Lentokoneiden viihdejärjestelmistä mainitaan Haassin ym. (2016) ja Standerin & Ophoffin (2016) tutkimuksissa. Standerin & Ophoffin (2016, 25–26) mukaan:

> *”Lentokoneiden viihdejärjestelmä ei välttämättä vaikuta todennäköiseltä ehdokkaalta kyberhyökkäykselle, mutta tarkempi tarkastelu osoittaa useita haavoittuvuuksia. Ensimmäinen näistä on se, että järjestelmä sisältää USB-portin matkustajien istuinten alapuolella. Nämä järjestelmät ovat myös kytkettyinä useisiin muihin laitteisiin, joihin sisältyy myös lentokoneen lennonhallintajärjestelmä. Vuonna 2013 lentokonevalmistaja Boeing anoi muutosta tyyppihyväksyntään tämän tyyppisen ongelman ratkaisemiseksi, joka osoittaa mahdollisuuden päästä luvattomasti käsiksi järjestelmiin, joko tahallisesti tai tahattomasti.” (Stander & Ophoff 2016, 25–26)*

Stander & Ophoff (2016, 26) lisäävät lentokoneiden viihdejärjestelmien käyttävän hyvin tunnettuja teknologioita, minkä vuoksi hyökkäysten toteuttamiseen vaadittava tieto on heidän mukaansa jo saatavilla. He kertovat vastaavien järjestelmien olevan myös muissa kuin Boeingin lentokonemalleissa. Haass ym. (2016, 43) listaavat viihdejärjestelmän uhkien kohteeksi, mutta eivät käsittele uhkia tarkemmin.

Miehittämättömät ilma-alukset voivat myös aiheuttaa uhkia kyberturvallisuudelle. Haassin ym. (2016, 40) mukaan testaus on osoittanut, että miehittämättömiä ilma-aluksia ohjaaviin GPS-signaaleihin voidaan saada etäyhteydellä pääsy, jonka avulla ilma-alusta voidaan ohjata

virheellisesti. Kessler & Craiger (2018, 24) mainitsevat miehittämättömien ilma-alusten uhkiksi GPS-signaalien väärentämisen, kontrollisignaalin sieppaamisen tai väärentämisen, videosignaalin sieppaamisen sekä antureiden häirinnän. Tämän lisäksi he tuovat esille mahdollisuuden haittaohjelmille maa-asemissa, palvelunestohyökkäykset sekä miehittämättömien ilma-alusten käytön terroristi-iskuissa (Kessler & Craiger 2018, 24).

Käytännössä synteesistä voidaan havainnoida, että miehittämättömiä ilma-aluksia voidaan mahdollisesti ohjata eri tavoin väärille reiteille, minkä seurauksena niillä voidaan aiheuttaa tuhoa johonkin valittuun kohteeseen. Videosignaalin sieppaamisella voidaan myös vakoilla tai kerätä tietoa jostakin valitusta kohteesta.

Kaiken kaikkiaan aineistossa käsiteltiin uhkia kohtuullisen epätodennäköisinä, mutta riskien toteutuessa niiden vaikutusten kyberturvallisuudelle voidaan havainnoida olevan korkeat. Voidaan myös arvioida luottamuksen menetyksen olevan todennäköinen seuraus laajasta tietovuodosta sekä kyberhyökkäyksestä ADS-B- tai GPS-järjestelmään, mikäli tällä aiheutettaisiin esimerkiksi lentokoneen törmäys maahan tai toiseen lentokoneeseen. Voidaan myös havainnoida uhkien vakiintumattomuus, sillä aineistojen erot uhkien tunnistamisen ja käsittelyn osalta ovat ilmeisiä. Tämä osoittaa tarpeen kyberriskin ja kyberturvallisuuden lisätarkastelulle siviili-ilmailussa.

5 KYBERRISKIEN SÄÄNTELY EUROOPAN SIVIILI-ILMAILUSSA

5.1 Kyberriskiä käsittelevät lait ilmailualalla

Euroopan komission (2018b) mukaan siviili-ilmailun sääntely mahdollistaa yhtäläisen matkustamisen turvallisuuden läpi Euroopan. Eurooppalainen lentoturvallisuusjärjestelmä pohjautuu yleisiin turvallisuusmääräyksiin, jotka kattavat sellaisenaan Euroopan unionin jäsenvaltioissa tapahtuvan siviili-ilmailun keskeiset alueet. Määräyksiä valvotaan Euroopan lentoturvallisuusvirasto EASA:n, Euroopan komission toimesta sekä kansallisten ilmailuviranomaisten toimesta. (Euroopan komissio 2018b) Euroopan lentoturvallisuus perustuu näin ollen pääosin

ajankohtaiseen ja tehokkaaseen sääntelyyn ja valvontaan (Euroopan komissio 2018c). Luvussa 4.1 käsitellysti ilmailuala keskittyy kyberriskiin yhä enemmän kyberturvallisuuden näkökulmasta, jossa keskiössä ovat kyberuhat. Sääntelystä voidaan havainnoida samoja merkkejä, sillä sääntelyssä keskitytään käytännössä kokonaisuudessaan vain kyberturvallisuuteen. Turvallisuussääntely ei niinkään arvioi tapahtumien vaikutusta tai todennäköisyyttä vaan keskittyy tapahtumien estämiseen kokonaisuudessaan.

Euroopan unionin sääntelyelinten keskittyminen myös kyberriskien olemassaoloon on huomattavissa Euroopan komission (2015b) ilmailustrategiasta alkaen. Ilmailustrategia Euroopalle asettaa suoran komission pyynnön Euroopan lentoturvallisuusvirastolle kyberriskien tutkimiseksi. Dokumentissa mainitaan ”Aivan kuten muidenkin lentoturvallisuuteen kohdistuvien riskien tapauksessa komissio pyytää Euroopan lentoturvallisuusvirastoa tutkimaan myös kyberriskejä…”. (Euroopan komissio 2015b) Komissio on siis nähnyt tarpeelliseksi tuoda kyberriskit esiin erillisenä riskinä kaikista muista, jotta niihin keskitettäisiin huomioita.

Euroopan ilmailustrategiassa komissio ehdottaa myös yhteisiä siviili-ilmailun sääntöjä säätäneen asetuksen 216/2008 korvaamista uudella asetuksella (Euroopan komissio 2015b). Uudistettu kyberriskit huomioiva Euroopan parlamentin ja neuvoston säätämä asetus 2018/1139 astui voimaan 11. syyskuuta 2018. Asetus koskee Euroopan unionin yhteisiä siviili-ilmailumääräyksiä sekä Euroopan lentoturvallisuusviraston perustamista. Asetuksella muutettiin Euroopan parlamentin ja neuvoston antamat asetukset 2111/2005, 1008/2008, 996/2010 ja 376/2014, sekä direktiivit 2014/30/EU ja 2014/53/EU. Asetuksella korvattiin Euroopan parlamentin ja neuvoston asetukset 552/2004, 216/2008 ja neuvoston asetus 3922/91. (Euroopan parlamentin ja neuvoston asetus 2018/1139) Asetuksella vastattiin Euroopan unionin vuonna 2015 vahvistamaan uuteen ilmailustrategiaan, jonka tarkoituksena on vastata tulevaisuuden haasteisiin ja kilpailuun (JAATO 2018b).

Vuodesta 1991 vuoteen 2014 annetut direktiivit ja asetukset eivät käsitelleet kyberriskiä tai kyberturvallisuutta. Asetuksessa 2018/1139 määrätään, että siviili-ilmailun sääntelyn tulisi vastata ”…niiden kohteena olevien eri ilma-alustyyppien ja muun toiminnan luonnetta ja riskejä, ja toimenpiteet olisi suhteutettava niiden luonteeseen ja riskeihin.” Sääntelytoimenpiteiden tulisi mahdollisuuden mukaan sallia ”…erilaisten keinojen käyttö näiden tavoitteiden saavuttamiseen…”, ottaen huomioon myös kyberturvallisuus. Erilaisten keinojen sallimisella

pyritään asetuksen mukaan teknisen ja operatiivisen innovoinnin edistämiseen alalla, sekä kustannustehokkuuteen turvallisuustasojen saavuttamisessa. (2018/1139)

Asetuksella pyritään parantamaan lentoturvallisuutta ja ennakoimaan uusia turvallisuusriskejä hyödyntäen rajallisia teknisiä resursseja parhaalla mahdollisella tavalla. Uusiin turvallisuusriskeihin on huomioitu myös kyberturvallisuus. Asetuksessa määrätään Euroopan lentoturvallisuussuunnitelman ja lentoturvallisuusohjelman laatimisesta. Suunnitelman tarkoituksena on vahvistaa Euroopan unionin turvallisuustaso ilmailualalle, jotta jäsenvaltiot voivat vahvistaa niiden vastuulla olevan ilmailutoiminnan hyväksyttävän turvallisuustason. Euroopan lentoturvallisuusohjelmaan tulee liittää ”…suunnitelma, jossa kuvaillaan toimet, jotka jäsenvaltio aikoo toteuttaa tunnistettujen turvallisuusriskien lieventämiseksi.” Asetuksessa halutaan varmistaa myös lennonvarmistusteknisen henkilöstön ja muiden lennonjohdon toimijoiden pätevyys- ja koulutustaso. Tämän osalta asetus määrää, että palveluiden tarjoajien ”…olisi myös toteutettava koulutus- ja tarkastusohjelmia ottaen huomioon henkilöstönsä hoitamat erityyppiset turvallisuuteen liittyvät tehtävät.” (2018/1139)

Asetus 2018/1139 määrää komission, Euroopan lentoturvallisuusviraston ja jäsenmaiden yhteistyöstä kyberturvallisuusasioissa, mikäli ”…siviili-ilmailun turvallisuuden ja turvatoimien välillä on keskinäisiä riippuvuussuhteita.”. Mikäli riippuvuussuhteita on, antaa Euroopan lentoturvallisuusvirasto komissiolle teknistä apua sekä reagoi ongelmaan antamalla suosituksia korjaavista toimista sekä jakamalla viranomaisille ja henkilöille tietoa asiasta. Viranomaisten, oikeushenkilöiden tai luonnollisten henkilöiden on toteutettava lentoturvallisuusviraston suositukset, mikäli niitä annetaan. (2018/1139)

Asetuksessa 2018/1139 huomioidaan siviili-ilmailun kasvava riippuvuus nykyaikaisesta tieto- ja viestintäteknologiasta, minkä vuoksi ”…olisi vahvistettava keskeiset vaatimukset siviili-ilmailualan käyttämien tietojen turvallisuuden varmistamiseksi.” Tämän lisäksi asetuksessa määrätään toimintamassasta riippumatta miehittämättömien ilma-alusten toiminnasta Euroopan alueella. Asetuksen mukaan ”Käyttäjän ja kauko-ohjaajan on kyettävä varmistamaan, että käyttö on turvallista ja että miehittämätön ilma-alus pysyy turvallisella etäisyydellä maassa olevista ihmisistä ja muista ilmatilan käyttäjistä.” Käyttäjän tulee myös olla tietoinen miehittämättömien ilma-alusten kansallisesta sääntelystä. Joidenkin miehittämättömien ilma-alusten täytyy ottaa myös huomioon sähkömagneettiset yhteensopivuudet ja radiotaajuudet,

jotta ne eivät aiheuta haitallisia häiriöitä. Osa miehittämättömistä ilma-aluksista tulee ilmoittaa kansalliseen rekisteriin asetuksen mukaan. (2018/1139) Esimerkiksi Suomessa käyttäjän tulee ilmoittaa liikennevirastolle kaikesta kauko-ohjatun ilma-aluksen toiminnasta. Alle 150 kilogramman miehittämättömiä ilma-aluksia ei rekisteröidä Suomen ilma-alusrekisteriin. (Trafi 2018d)

Asetuksella 2018/1139 halutaan myös helpottaa riskien yksilöintiä, arviointia ja lieventämistä tiedon jakamisen avulla. Tämän vuoksi asetus määrittää, että ”…komission, viraston ja kansallisten toimivaltaisten viranomaisten olisi vaihdettava kaikkia käytettävissään olevia tietoja tätä asetusta soveltaessaan.” Euroopan lentoturvallisuusviraston on asetuksen mukaan ”…osallistuttava yhteistyöhön ilmailun turvatoimien alalla, kyberturvallisuus mukaan luettuna.” Tietoon keskitytään jakamisen lisäksi suojaamisen osa-alueella. Asetuksella vahvistetaan viranomaisten keräämien tietojen ja tietolähteiden suojaaminen sekä luodaan sähköinen rekisteri osapuolten tiedonvaihdon varmistamisen vuoksi. Asetuksenmukaisten henkilötietojen käsittelyyn sovelletaan Euroopan yleistä tietosuoja-asetusta. (2018/1139)

Euroopan lentoturvallisuusvirasto on tehnyt määräajoin lentoturvallisuussuunnitelmia lisätäkseen siviili-ilmailun turvallisuutta Euroopan alueella. Vuosien 2014–2017 suunnitelmassa kyberriskiä tai kyberturvallisuutta ei mainittu, mutta uusien teknologioiden, järjestelmien ja toimintatapojen riskialue mainittiin nousevana uhkana. (EASA 2014) Vuosien 2016–2020 suunnitelmassa kyberriskiä käsiteltiin kyberturvallisuuden kautta osana uusien teknologioiden, järjestelmien ja toimintatapojen riskialuetta. Uusi suunnitelma osoittaa myös Euroopan lentoturvallisuusviraston harkitsevan lentokoneiden kyberturvallisuuteen tähtäävää direktiivimuutosta katselmuksella RMT.0648. (EASA 2016a) Katselmuksessa tarkistetaan turvallisuussääntöjä sääntelykehikon luomiseksi. Sääntelykehikolla on tarkoitus tunnistaa turvallisuuteen vaikuttavia kyberriskejä ja vähentää niitä. Erityisenä pääpainona katselmuksessa on lentokoneen sähköisten verkkojen ja järjestelmien laiton häirintä. (EASA 2016b) Euroopan lentoturvallisuusviraston verkkosivujen mukaan direktiivimuutoksia katselmuksen pohjalta ei ole vielä tehty, eikä hakemistosta löydy jatkotoimenpiteitä vuoden 2016 katselmukselle.

Katselmuksen RMT.0648 tarkoituksena on ajaa uusien standardien kehittämistä, sillä katselmuksen mukaan kyberturvallisuutta varten ei ole tehty omia standardeja. Katselmuksen mu-

kaan kyberriskiä tarkastellaan kyberturvallisuuden näkökulmasta standardin 21A.16B erityisehdon kautta lentokonetta sertifioidessa. Tämä erityisehto ottaa huomioon turvallisuuden varmistusprosessin, jolla eristetään tai suojataan lentokonejärjestelmiä ja verkkoja ulkoisilta ja sisäisiltä turvallisuusuhkilta. Sääntely vaatii lentokonejärjestelmien arvioinnin mahdollisten virheitä aiheuttavien tietoturvallisuusuhkien varalta. Katselmus ehdottaa useiden sertifiointien uudistamista kyberturvallisuuden huomioimiseksi. Katselmuksessa mainitaan Euroopan lentoturvallisuusviraston suunnittelevan sääntelyn yhdenmukaistamista Yhdysvaltain lentoturvallisuusviraston kanssa. Yhdysvaltain lentoturvallisuusvirasto kehitti vuonna 2015 sääntelyä lentokoneiden tietojärjestelmien suojaamiseksi. (EASA 2016c) Sertifiointimuutoksia ei Euroopan lentoturvallisuusviraston verkkosivujen hakemiston mukaan ole vielä tehty, eikä yhdenmukaistamista Yhdysvaltain sääntelyn kanssa kyberturvallisuuden osalta ole vielä tehty.

Euroopan lentoturvallisuusviraston vuosien 2018–2020 lentoturvallisuussuunnitelman mukaan Euroopan lentoturvallisuusvirasto on perustanut vuonna 2017 eurooppalaisen ilmailun kyberturvallisuuskeskuksen yhteistyössä Euroopan tietokoneiden hätätilavalmiusryhmä CERT-EU:n kanssa. Valmiusryhmästä käytetään lyhennettä ECCSA. Perustetun keskuksen tehtävänä on toimia tiedon jakajana ja toimialan toimijoiden yhteistyökumppanina kriittisten osa-alueiden, kuten valvonta- ja navigointijärjestelmien sekä datalinkkien turvaamiseksi. Suunnitelman mukaan tässä luvussa edellä käsitelty RMT.0648 katselmus etenee päätettäväksi vuonna 2019. Tämän lisäksi suunnitelma listaa toisen katselmuksen RMT.0720, jolla aiotaan luoda sääntelyjärjestelmä ilmailujärjestelmien suojaamiseksi kyberhyökkäyksiltä ja niiden seuraamuksilta. Sääntelyn tarkoituksena on kattaa koko ilmailun toimiala suunnittelusta ja valmistamisesta operointiin asti. Suunnitelman mukaan katselmuksen olisi ollut määrä ilmestyä vuoden 2017 neljännellä kvartaalilla. Päätös muutoksista arvioidaan tapahtuvan vuonna 2020. (EASA 2017) Euroopan lentoturvallisuusviraston hakemistosta ei löydy RMT.0720 katselmusta, eikä lisätietoa sen etenemisen vaiheista tai sääntelymuutosprosessin aloittamisesta.

Sääntelystä voidaan havainnoida kyberriskien huomioiminen kyberturvallisuutena, jolloin kyberriskiä halutaan estää kokonaisuudessaan. Sääntelyä kyberriskien pohjalta on kuitenkin Euroopan tasolla verrattain vähäisesti ja se vaikuttaa tällä hetkellä olevan hyvin yleisluontoista tai suunnittelevaa, eikä konkreettisia toimia kyberriskien torjumiseksi mainita sääntelyssä. Wuolijoen (2016, 2) mukaan yleisluontoinen sääntely siirtää valtaa lain tulkintavirkamiehille, joka on ongelmallista vallanjako-oppien näkökulmasta.

5.2 Kyberriskiä käsittelevät standardit ja suositeltavat käytännöt

Lain lisäksi siviili-ilmailussa suurina toimijoina toimivat luvussa 3.3.4 esitellyt järjestöt, jotka suosittavat usein jäseniään ottamaan käyttöön järjestöjen standardit ja suositellut käytännöt. Luvussa 3.3.4 mainitusti Kansainvälinen siviili-ilmailujärjestö julkaisee standardeja ja suositeltuja käytäntöjä, jotta jäsenvaltiot voivat hyväksyä ne osaksi lainsäädäntöään. Mikäli niitä ei vahvisteta lainsäädännössä, julkaistaan poikkeukset järjestön toimesta kansainvälisesti tarkasteltavaksi. Järjestöjen työllä voidaan havainnoida historiallisesti olleen vaikutusta sääntelyn muodostumiseen, jonka vuoksi niitä käsitellään tässä luvussa.

Euroopan lentoturvallisuusvirasto tekee yhteistyötä Kansainvälisen siviili-ilmailujärjestön kanssa. Euroopan lentoturvallisuusvirasto auttaa muun muassa jäsenmaitaan implementoimaan Kansainvälisen siviili-ilmailujärjestön standardeja sekä vaihtaa turvallisuustietoja Kansainvälisen siviili-ilmailujärjestön kanssa. (EASA 2018c) Kansainvälinen siviili-ilmailujärjestö julkaisi vuonna 2011 liitteen ”Annex 17” kymmenennen version, joka käsittelee myös kyberuhkia. Liitteessä käsitellään standardien ja suositeltujen käytäntöjen päivittämistä muun muassa kyberuhkien huomioimiseksi. Kyberuhkiin vastaamiseksi liitteeseen on liitetty suosituksia, joiden mukaan järjestö suosittaa jäsenvaltioitaan kehittämään toimintoja kriittisten tieto- ja kommunikointijärjestelmien suojaamiseksi ulkoiselta häirinnältä. Tämän lisäksi liitteessä suositetaan näiden järjestelmien sekä niitä koskevien uhkien ja haavoittuvuuksien tunnistamista, sekä vastatoimien kehittämistä järjestelmien suojaamiseksi. (ICAO 2011) Suositukset eivät kuitenkaan ole sitovia, minkä vuoksi ne eivät velvoita jäsenvaltioita sellaisenaan.

Järjestö julkaisi lisäksi vuonna 2016 päätöksen A39–19, jolla kehotetaan valtioita ja alan sidosryhmiä tunnistamaan toiminnan ja kriittisten järjestelmien kyberuhkia ja -riskejä aikaisempien tapahtumien avulla sekä vastaamaan niihin. Tämän lisäksi päätös kehottaa valtioita ja alan sidosryhmiä muun muassa määrittämään kyberturvallisuuden osalta kansallisten toimijoiden vastuut, luomaan yhteisymmärryksen kyberuhkista ja -riskeistä, luomaan kriteerit järjestelmien kriittisyyden määrittelemiseksi, ottamaan käyttöön kyberturvallisuusjärjestelmiä sekä määrittämään oikeudelliset seuraukset kyberturvallisuuden vaarantamisesta. (ICAO 2016)

Päätöksestä voidaan havainnoida lisästandardien ja -käytäntöjen tekemisen halukkuus kyberriskien torjumiseksi tulevaisuudessa, mutta päätös tuo myös esille selvän tiedon puutteen riskeistä, minkä vuoksi riskejä pyydetään tunnistamaan ja tietoa välittämään. Päätös tuo myös esille vakiintumattoman käytännön kyberturvallisuuden osalta, sillä päätöksestä voidaan havainnoida, ettei suurimmassa osassa jäsenvaltioita ole määritelty vastuita tai oikeudellisia seurauksia kyberturvallisuusasioiden osalta.

Lentoyhtiöiden liittoumajärjestö The International Airline Traffic Association on myös julkaissut asemansa kyberturvallisuudesta vuonna 2015 tunnistaen kyberriskien ja -uhkien mahdollisen merkittävän vaikutuksen alan tulevaisuudelle. Julkaisussa järjestö ehdottaa muun muassa yhteistyön lisäämistä kyberriskien lieventämiseksi, käytäntöjen tekemistä ja jakamista kyberriskien lieventämiseksi sekä sietokyvyn lisäämiseksi alalla, potentiaalisten kyberriskien jatkuvan valvonnan tukemista järjestön osalta sekä sääntelyn edistämistä hallituksille ja alan sääntelijöille älykkäämmän sääntelyn luomiseksi. (IATA 2015) Julkaisusta voidaan havainnoida sekä kyberriskiä koskevien käytäntöjen että kyberriskien tiedon puute myös toimijoiden osalta.

Lentoyhtiöiden liittoumajärjestön mukaan Euroopan hallitustenvälinen järjestö European Civil Aviation Conference on vuodesta 2010 lähtien kehittänyt uusia suosituksia ja ohjemateriaalia kyberriskistä johtuen (IATA 2015). Suosituksia ei ole julkaistu järjestön sivustoilla (ECAC 2018c). Lentoyhtiöiden liittoumajärjestö mainitsee myös lennonjohdon toimijoita edustavan organisaatio Civil Air Navigation Services Organisationin julkaisseen kyberturvallisuus ja -riskiohjeen lennonjohdon toiminnan tueksi sekä mainitsee lentoyhtiöiden liittoumajärjestön kehittämän kolmipilarisen strategian, joka kattaa kyberriskien hallinnan, puolustautumisen, raportoinnin ja kommunikoinnin. (IATA 2015) Järjestö ei mainitse julkaisussa tehtyjä toimia sääntelyn edistämiseksi kyberriskien osalta.

5.3 Muu kyberriskiä käsittelevä sääntely

Tässä luvussa esitellään kyberriskiä käsittelevä sääntely, jota ei ole tehty vain siviili-ilmailun toimialalle, mutta se vaikuttaa siviili-ilmailun toimintaan. Tiedon suojaamisen merkitys on noussut myös esiin Euroopan unionin lainsäädännössä. Vuonna 2016 julkaistu ja vuoden 2018

toukokuussa voimaan astunut uusi tietosuoja-asetus koski myös siviili-ilmailun toimijoita Euroopassa. Euroopan parlamentin ja neuvoston asetuksella 2016/679 säädettiin ”…luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta…” (Euroopan parlamentin ja neuvoston asetus 2016/679).

Euroopan alueiden lentoyhtiöliitto ERA:n mukaan (2018) kyseessä on suurin Euroopan unionin 20 vuoteen antama lainsäädäntö, joka astuu voimaan sellaisenaan kaikissa Euroopan unionin jäsenmaissa. Lentoyhtiöliiton mukaan lakiuudistus ottaa huomioon digitaaliset ja verkkoalustat, joita aikaisempi lainsäädäntö ei huomioinut ottaen kantaa muun muassa suostumukseen, profilointiin, yksilön oikeuksiin, tietojenkäsittelijöiden velvoitteisiin, tietomurtoihin ja kyberhyökkäyksiin. Liitto kritisoi asetuksen kompleksisuutta ja kertoo sen sisältävän raskaita vaatimuksia lentoyhtiöille. (ERA 2018) Asetuksessa määrätään ilmoittamaan muun muassa tietojen keräämisestä ja käsittelystä palvelun tai sivuston käyttäjälle. Tietomurroista tulee asetuksen mukaan ilmoittaa viranomaiselle ilman aiheetonta viivästystä. (2016/679)

Asetuksen kohta 37(1) vaatii tietosuojavastaavan nimittämistä tilanteissa, joissa muun muassa ”…rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa…”. (2016/679) Euroopan alueiden lentoyhtiöliitto kertoo lentoyhtiöiden liittoumajärjestö IATA:n suosittavan jäsenilleen tietosuojavastaavan nimittämistä. (ERA 2018)

Vuonna 2016 julkaistiin myös Euroopan parlamentin ja neuvoston direktiivi 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko Euroopan unionissa. Direktiivin mukaisesti perustetaan myös verkosto tietoturvahäiriöiden vastausryhmiä, jotka muodostuvat Euroopan tietotekniikan kriisiryhmän ja tietoturvahäiriöiden vastausryhmien toimijoiden edustajista. Verkosto perustetaan, ”Jotta voidaan edistää luottamuksen kehittämistä jäsenvaltioiden välillä sekä edistää ripeää ja tehokasta operatiivista yhteistyötä…”. Tämän lisäksi direktiivi velvoittaa jäsenmaita tekemään ”…verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia…” ja ”…nimettävä yksi tai useampi verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen…”. (Euroopan parlamentin ja neuvoston direktiivi 2016/1148)

Kansainvälisen siviili-ilmailujärjestön konferenssissa tuotiin esille direktiivin 2016/1148 vaativan merkittävien tapahtumien ilmoitusta viranomaisille keskeisten palveluiden tarjoajien osalta (ICAO 2018d). Valtioneuvoston (2017) mukaan direktiivi velvoittaa jäsenvaltiot määrittämään nämä keskeiset palveluntarjoajat. Määritettyjen palveluntarjoajien tulee saada tieto siitä, että heidät on määritelty direktiivin mukaisesti keskeisiksi palveluntarjoajiksi. Valtioneuvoston mukaan lentoliikenne on direktiivin mukainen toimiala, jonka vuoksi direktiivi määrittelee alan keskeisille palveluntarjoajille ”…vähimmäisvelvoitteet korkean verkko- ja tietojärjestelmien turvallisuuden ylläpitämiseksi. Jäsenvaltiot voivat ottaa käyttöön myös direktiiviä pidemmälle meneviä oikeuksia ja velvoitteita. Direktiivin luonteesta johtuen ei kuitenkaan ole täysin selvää, mitä on pidettävä direktiivin vähimmäisvelvoitteina. Esimerkiksi jäsenvaltioiden on määriteltävä keskeiset palvelut direktiivin määrittämillä toimialoilla. Jäsenvaltioille on annettu suhteellisen laaja harkintavalta siinä, mitä nämä palvelut ovat.” (Valtioneuvosto 2017) Tämän voidaan havainnoida johtavan erilaisiin vaatimuksiin eri jäsenmaissa, mikä voi olla ongelma sääntelyn yhtenäisyyden ja selkeyden kannalta. Osa valtioista saattaa täyttää direktiivin määräykset vain minimitasolla, mikä voi aiheuttaa kyberriskien järjestelmästä toiseen liikkuvan luonteen vuoksi uhkia ja haavoittuvuuskohtia myös hyvin varautuneille valtioille.

Aikaisemmin mainittu sääntelyn yleisluontoisuuden ongelmallisuus vaikuttaa pätevän myös tässä luvussa käsiteltävään sääntelyyn, sillä suuri osa direktiivin 2016/1148 tulkinnasta vaikuttaa siirtyneen jäsenvaltioille. Wuolijoen mukaan (2016, 2) yleisluontoinen sääntely siirtää valtaa lain tulkintavirkamiehille, mikä on ongelmallista vallanjako-oppien näkökulmasta. Kyberriskien torjumisen sääntely kyberturvallisuuden kautta on myös jakautunut useisiin eri asetuksiin ja direktiiveihin. Tämän lisäksi uutta sääntelyä on tullut lähivuosina Euroopan tasolla verrattain nopeasti ja muutoksia sääntelyyn on koettu lähivuosina useaan otteeseen. Liian laaja tai jatkuvasti muuttuva sääntely voi Wuolijoen (2016, 2) mukaan estää sääntelyn selvyyden ja selonoton, tehden sääntelystä oikeusturvan kannalta kestämätöntä.

5.4 Valvonnan muutos

Valvonta jakautuu luvussa 3.5 käsitellysti jäsenvaltioiden, Euroopan lentoturvallisuusviraston ja Euroopan komission välille viraston valvoessa laajinta osa-aluetta siviili-ilmailun toiminnasta. (Euroopan komissio 2015a) Sääntelyn muutos on vaikuttanut siviili-ilmailun toimijoiden lisäksi alan valvontaan, minkä vuoksi siviili-ilmailussa on alettu kehittämään Euroopan lentoturvallisuusviraston toimesta riskipohjaista valvontaa (EASA 2016d). Valvonnan pohja on sääntelyssä, minkä vuoksi myös valvonnan muutos voidaan nähdä sääntelyn muutoksena kyberriskien tietoisuuden johdosta.

Kansainvälisen siviili-ilmailujärjestön liite 19 määrittää, että valvontaa on siviili-ilmailussa harjoitettava ”…suuremman turvallisuuden tai tarpeen alueilla.” Liite on osa Chicagon yleissopimusta, joka sitoo kaikkia Euroopan unionin jäsenmaita (2018/1149). Euroopan ilmailuviraston dokumentissa mainitaan, että lentoturvallisuusviraston soveltamissäännöt esittelevät riskipohjaisen valvonnan jokaisella siviili-ilmailun osa-alueella lennonjohdosta lentoyhtiöihin tehokkaamman valvonnan aikaansaamiseksi. Toistaiseksi ohjeita ei kuitenkaan ole tarpeeksi sujuvan ja yhtenäisen vaatimusten toteuttamisen varmistamiseksi. Tämän vuoksi Euroopan ilmailuvirasto on julkaissut vuonna 2016 dokumentin, joka listaa käytäntöjä riskipohjaisen valvonnan toteuttamiseksi. Nämä eivät kuitenkaan dokumentin mukaan ole suoraa verrattavissa sääntelyyn, vaan ehdottavat toistaiseksi käytäntöjä. (EASA 2016d) Tämän vuoksi niitä ei käsitellä tässä luvussa tarkemmin, vaan dokumentin esittelyllä pyritään osoittamaan valvonnan muutoksen tarpeellisuus tulevaisuudessa.

Valvonnan sääntelyn muuttamiseen menee kuitenkin todennäköisesti useita vuosia, mikäli tulevia sääntelymuutoksia arvioidaan sen perusteella, kuinka kauan aikaisempien merkittävien muutosten tekemiseen on Euroopan unionilta mennyt. Riskipohjaisesta valvonnasta voidaan havainnoida, ettei nykyinen valvonnan sääntely osoita tarpeellista huomioita kaikille riskeille valvonnan osalta. Sääntelyssä kyberriskit on huomioitu kyberturvallisuuden kautta ja niistä on mainittu lisänä lausekkeen lopussa. Tästä voidaan havainnoida, että kyberriskejä ei välttämättä ole otettu huomioon valvojien mielestä tarpeeksi. Kyberriskit ovat toimineet merkittävänä osana sysäämään riskipohjaisen valvonnan käytännön kehittämistä.

Asetuksessa 2018/1139 määrätään, että ”Avoimuuden vuoksi niiden, joita asia koskee, olisi voitava saada tarkkailijan asema viraston hallintoneuvostossa.” Tämän lisäksi asetuksessa mainitaan, että yleisen edun vuoksi Euroopan lentoturvallisuusviraston turvallisuustoimet perustuvat riippumattomaan asiantuntemukseen. Asetuksessa määrätään myös muutoksenhakukeinot, joilla halutaan varmistaa niiden osapuolten oikeudet, joita viraston tekemät päätökset koskettavat. Asetuksen mukaan on myös ”…tarpeen antaa yleisölle riittävästi tietoja siviili-ilmailun turvallisuustasosta…”. (2018/1139) Toimista voidaan havainnoida Euroopan unionin haluavan varmistaa sääntelyn läpinäkyvyyttä. Euroopan unionin kaikissa asetuksissa ja direktiiveissä pidetään yleisesti saman tason läpinäkyvyydestä kiinni. Turvallisuustoimien perustuminen riippumattomuuteen asiantuntemukseen voi kuitenkin aiheuttaa luvussa 3.2 käsitellyn läpinäkymättömyyden ongelman, jolloin julkisesti sääntelyn tarkastelu on vaikeaa ilman asiantuntijoiden selityksiä. Riittävien tietojen antamisella yleisölle ja tarkkailijan asemalla viraston hallintoneuvostossa varmistetaan, että läpinäkyvyys sääntelyssä kuitenkin säilyy kohtuullisella tasolla.

Asetus 2018/1139 ottaa myös kantaa sakottamiseen asetuksen nojalla. Asetuksen mukaan ”…asetuksen noudattamisen varmistamiseksi olisi viraston antamien todistusten haltijoille ja ilmoituksen virastolle antaneille yrityksille voitava määrätä sakkoja tai uhkasakkoja tai molempia, jos ne rikkovat niihin tämän asetuksen nojalla sovellettavia sääntöjä. Komission olisi määrättävä tällaiset sakot ja uhkasakot viraston suosituksen perusteella.” Sakkoihin ei ole yksioikoista ohjetta, vaan ne sisältävät aina harkintavaltaa olosuhteet huomioon ottaen. (2018/1139) Asetuksessa 2016/1138 ei puolestaan määrätä sakottamisesta.

Tietosuoja-asetuksessa 2016/679 määrätään sakottamisesta sääntöjen rikkomistilanteessa täytäntöönpanon varmistamiseksi. Sakkojen sijaan asetuksen 2016/1138 rikkomistilanteessa voidaan antaa myös huomautuksia. Asetuksen laajuuden vuoksi sakkojen antamisoikeus on laajennettu jokaiselle asetuksen valvontaviranomaiselle. Asetuksen mukaan ”Hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti…” ja rikkomistilanteissa pitää ottaa huomioon esimerkiksi rikkomisen vakavuus, kesto, luonne, tahallisuus tai tuottamuksellisuus, lieventämistoimet, vastuun aste, aiemmat rikkomukset ja rikkomuksen ilmenemistapa. Hallinnollisen sakon enimmäismäärä on 10 miljoonaa euroa tai yrityksen tilanteessa ”…kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonais-

liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi…” Sakko voi olla myös enimmäismäärältä 20 miljoonaa euroa tai neljä prosenttia edellä mainitusta kokonaisliikevaihdosta, mikäli rike koskee henkilötietojen siirtoa kolmanteen maahan, käsittelyn perusperiaatteita tai erityistilanteita, kuten kansallisen henkilötunnuksen käsittelyä. (2016/679)

Tästä voidaan havainnoida, että toimilla koetetaan turvata tietojenkäsittelyä Euroopan unionissa ja korotetuilla sakoilla koetetaan pitää tiedot Euroopan unionin alueella, jotta tietoja voidaan suojata lainsäädännön mukaisesti. Luvussa 2.5 käsitellysti toteutuneiden kyberriskien vastuita tai vahingonkorvauksellisuutta voi olla vaikea määrittää. Sakottaminen luo selkeän vastuun, mikäli tietoja käsitellään asetuksen vastaisesti. Tämä konkretisoi yrityksille tietojen käsittelyn tärkeyden ja estää vastuun pakenemista.

6 JOHTOPÄÄTÖKSET JA YHTEENVETO

6.1 Tutkimusongelmiin vastaaminen

Tutkielman ensimmäisellä tutkimusongelmalla pyrittiin vastaamaan siihen miten kyberriskit voivat vaikuttaa siviili-ilmailun kyberturvallisuuteen. Vastausta lähdettiin selvittämään systemaattisen kirjallisuuskatsauksen aineistosynteesillä, johon valittiin aineistossa esiintyvät vaikutuskohteet ja niitä koskevat uhkat. Eniten esiintyneitä löydöksiä analysoitiin tarkemmin. Eniten aineistossa esiintynyt uhka oli etähyökkäys, jonka lisäksi aineistossa huomioitiin tahalliset ja tahattomat virheet, laitteiston häiriöt, lähihyökkäykset, haittaohjelmat ja koulutusviive. Uhkien vaikutusten pahentajana huomioitiin myös sää tai muut ulkoiset olosuhteet.

Kyberriskejä luokiteltiin luvussa 2.2. Kyberriskit luokiteltiin ihmisten toimintaan, järjestelmähäiriöihin ja teknologisiin vikoihin, epäonnistuneisiin sisäisiin prosesseihin sekä ulkoisiin tapahtumiin. Havaitut uhkat voidaan jakaa näihin kategorioihin. Etä- ja lähihyökkäykset sekä tahalliset ja tahattomat virheet kuuluvat ihmisten toiminnan kategoriaan. Laitteiston häiriöt voidaan puolestaan sijoittaa järjestelmähäiriöihin ja teknologisiin vikoihin. Haittaohjelmat jakautuvat ihmisten toiminnan sekä järjestelmähäiriöiden ja teknologisten vikojen kategoriaan, sillä

niiden kehittäminen vaatii ihmisen tahallista toimintaa, järjestelmään tartuttaminen tahallista tai tahatonta toimintaa ja häiriön aiheutuminen turvallisuusasetuksien heikkoutta tai laitteiston vanhentuneisuutta. Koulutusviive sijoitetaan epäonnistuneiden sisäisten prosessien kategoriaan. Sää tai muut ulkoiset olosuhteet luokitellaan ulkoisten tapahtumien kategoriaan. Voidaan siis havainnoida jokaisen operationaalisten kyberriskien kategorian vaikuttavan siviili-ilmailun kyberturvallisuuteen.

Taulukoiden vertailusta voidaan päätellä, että kyberriskeistä ihmisten toiminta vaikuttaa selvästi laajimmin siviili-ilmailun kyberturvallisuuteen. Järjestelmähäiriöiden ja teknologisten vikojen vaikutus on toiseksi suurin. Kolmannelle jaetulle sijalle asetetaan ulkoisten tapahtumien ja epäonnistuneiden sisäisten prosessien kategoriat. Ihmisten toiminnasta tahallinen toiminta vaikuttaa eniten, sillä aineistosta voitiin analysoida lähi- ja etähyökkäysten vaikuttavan laajimmin kyberturvallisuuteen. Hyökkäysten kohteiden ja vaikutusten laaja-alaisuus lisäävät uhkan merkittävyyttä. Hyökkäysten todennäköisyys arvioitiin kuitenkin yleisesti matalaksi, minkä vuoksi tässä tutkielmassa niiden kokonaisvaikutus kyberturvallisuuteen on arvioitu maltilliseksi.

Järjestelmähäiriöiden todennäköisyys arvioitiin yleisesti hyökkäysten todennäköisyyttä hieman korkeammaksi. Niiden laajuus ei kuitenkaan ollut yhtä kattava kuin mahdollisten hyökkäysten, minkä vuoksi järjestelmähäiriöiden vaikutus kyberturvallisuudelle voidaan myös arvioida maltilliseksi aineiston pohjalta. Kerroinvaikutusten arviointi aineiston perusteella on hankalaa. Luvussa 2.1 käsitellysti kyberriski on kuitenkin vahvasti korreloiva riski, jonka vuoksi kerroinvaikutusten voidaan olettaa vaikuttavan yleisesti jokaiseen kyberriskiin. Tämä lisää ulkoisten tapahtumien ja epäonnistuneiden sisäisten prosessien kategorioiden merkitystä. Hyökkäyksen tai virheen aiheuttama epäselvyys voi johtaa vääriin toimiin, jotka voivat vaikuttaa riskiä lisäävällä tavalla. Ulkoiset tekijät voivat lisätä riskin aiheuttaman epäselvyyden vaikutusta.

Hyökkäyksistä todennäköisimmiksi arvioitiin GPS- ja ADS-B-järjestelmien väärennetyt signaalit ja häirintähyökkäykset. Todennäköisyyttä järjestelmien hyökkäyksille lisäsi niiden heikko salaustaso, tunnistautumisen protokollan puuttuminen ja tiedon yleinen saatavuus julkisilta verkkosivustoilta. Väärennetyt signaalit arvioitiin vakavammiksi kuin palvelunestohyökkäyk-

set niiden vaikean tunnistettavuuden vuoksi. GPS-signaalien väärentäminen arvioitiin epätodennäköisemmäksi kuin ADS-B järjestelmän signaalien väärennys. Laajaskaalaisten häirintähyökkäysten toteuttaminen arvioitiin vaikeaksi.

GPS-järjestelmän palvelunestohyökkäyksiä arvioitiin eriävin mielipitein. Palvelunestohyökkäysten arvioitiin olevan sekä vaikeita että helppoja toteuttaa. Palvelunestohyökkäysten vaikutusten arvioitiin olevan vakavia, mutta uhkan vakavuutta lieventää sen hyväksi arvioitu tunnettuus alalla sekä usean samanaikaisen navigointijärjestelmän käyttö.

ADS-B-järjestelmän viestien tahallisen peukaloinnin todennäköisyydeksi arvioitiin sekä keskitaso että matala taso. Peukaloinnin turvallisuusvaikutusten arvioitiin olevan merkittäviä, mutta ei erityisen merkittäviä. Viestin peukaloinnin vakavuutta lisää niiden tunnistamisen vaikeus, mutta peukaloinnin arvioitiin olevan vaikeaa. Järjestelmän signaalin tahallinen viivästyttäminen arvioitiin todennäköisyydeltään matalaksi ja vaikutukseltaan lieväksi. Viivästyttämisen estäminen arvioitiin kustannusten vuoksi kuitenkin erittäin hankalaksi. Järjestelmän tahallinen sammuttaminen arvioitiin erittäin vakavaksi uhkaksi, mutta tapahtuman todennäköisyyden arveltiin ymmärrettävästi olevan todella matala.

Aineistossa arvioitiin tietokanavan häiriöistä bittivirhesuhteen olevan todennäköisin uhka ja sen arvioitiin aiheuttavan erittäin merkittäviä turvallisuusvaikutuksia. Bittivirhesuhde voi estää signaalien vastaanoton. Vain yksi tutkimus oli kuitenkin huomioinut uhkan, jonka vuoksi sen merkittävyyttä yleisellä tasolla on vaikea arvioida. Myös maa-aseman vahingoittamista tai manipulointia sekä koulutusviivettä arvioitiin vain yhdessä tutkimuksista, minkä vuoksi yleistävien havaintojen tekeminen ei niiden osalta ole mahdollista.

ADS-B- ja GPS-järjestelmien puutteista ei ollut laajaa tietoisuutta alan toimijoiden keskuudessa. ADS-B-järjestelmän ongelmien arvioitiin olevan huolestuttavia sen suunnitellun käytön merkittävyyden vuoksi. Näin ollen voidaan havainnoida ADS-B-järjestelmään kohdistuvien kyberriskien vaikuttavan eniten kyberturvallisuuteen. Riskien toteutuminen voi aiheuttaa epäselvyyttä toimijoissa ja virheellisen toiminnan kerroinvaikutuksen kautta ongelmat voivat johtaa viivästymisiin tai jopa onnettomuuksiin.

ACARS-järjestelmän merkittävimmiksi uhkiksi arvioitiin hyökkäyksen avulla toteutettu tietomurto sekä väärennetyt signaalit. Tietomurron todennäköisyyttä lisää järjestelmän yleisesti

todettu erittäin heikko salaus ja tietojen osittainen saatavuus verkkosivustojen kautta. Tietomurron vakavuutta lisää sen kautta lähetettävien viestien sisältö, sillä järjestelmän kautta lähetetään turvallisuudelle kriittistä tietoa lentokoneesta, matkustajista ja henkilökunnasta. Vakavuuden ja todennäköisyyden lieventämiseksi on kuitenkin tehty toimia, kuten viestien sisältöjen koodaamista ja järjestelmän käyttämättä jättämistä. Väärennetyt signaalit voivat aiheuttaa epäselvyyksiä, minkä seurauksena virheelliset toimet voivat alentaa turvallisuutta. Järjestelmää kohtaavat kyberriskit voivat näin ollen vaikuttaa kyberturvallisuuteen aiheuttamalla turvallisuuden alentumista, viivästymisiä sekä tietomurtoja. Tietomurrot ja viivästymiset voivat vaikuttaa siviili-ilmailun luotettavuuteen, joka on Limnéllin (2014, 40) mukaan merkittävä osa kyberturvallisuutta.

Henkilökuntaan liittyvistä sisäpiirin uhista mainittiin aineistossa vähäisesti. Tahallinen lentokoneen törmäämisen aiheuttaminen voitaisiin luokitella Haassin ym. (2016) mukaan myös kyberriskiksi. Tapahtuman todennäköisyyden voidaan havainnoida olevan erittäin matala. Ihmisten hyvällä hallinnoinnilla voidaan myös pitää riskin todennäköisyys matalana. Kerroinvaikutuksena käsitellyt turvattomat päätökset voidaan nähdä myös henkilökunnan kategorian uhkana. Niiden vaikutus on liitännäisenä muihin riskeihin, minkä vuoksi niiden ei havainnoida olevan itsenäisenä uhkana kovin merkittävä. Henkilökunnan riskit voivat näin ollen vaikuttaa merkittävästi kyberturvallisuuteen aiheuttamalla jopa onnettomuuksia, mutta niiden todennäköisyys on häviävän pieni, minkä vuoksi riskejä ei kokonaisuudessaan voida pitää merkittävinä kyberturvallisuuden kannalta.

Lentohenkilökunnan omia laitteita aineisto käsitteli epämääräisesti, mainiten vain elektronisen lentäjälaukun. Tämän lisäksi aineistossa mainittiin, että joihinkin laitteisiin voitaisiin ladata haittaohjelmia, jotka tarttuisivat laitteista järjestelmiin. Laitteisiin liittyviä riskejä ei kuitenkaan voida arvioida aineiston epämääräisyyden vuoksi. Voidaan kuitenkin tulkita, ettei laitteiden turvallisuusvaikutuksista ole vielä selkeää kuvaa.

Lentokoneen viihdejärjestelmää pidettiin mahdollisena, muttei todennäköisenä hyökkäyskohteena. Järjestelmän kautta toteutettava lähihyökkäys voisi antaa hyökkääjälle pääsyn lentokoneen lennonhallintajärjestelmään. Riski lähihyökkäykselle on siis mahdollisesti olemassa, mutta sen todennäköisyyttä tai vaikutuksia ei ole aineistossa arvioitu, minkä vuoksi sen vaikutusta kyberturvallisuudelle ei voida määrittää.

Miehittämättömissä ilma-aluksissa ongelmaksi tunnistettiin ohjaamiseen käytettävä GPS-järjestelmä, johon pätee kaikki aiemmin käsitellyt GPS-järjestelmän ongelmat, kuten signaalin väärentäminen, sieppaaminen ja häirintä. Järjestelmän heikkoudet altistavat miehittämättömät ilma-alukset kaappauksille, joiden avulla niitä voitaisiin käyttää hyökkäyksen välineenä. Ilma-aluksella voitaisiin näin ollen törmätä tahallisesti lentokoneeseen tai muuhun kohteeseen, aiheuttaen merkittäviä turvallisuusvaikutuksia. Riskin todennäköisyyttä ei kuitenkaan ole aineistossa arvioitu. Tämän vuoksi voidaan todeta riskin voivan aiheuttaa vaikutuksia kyberturvallisuudelle, mutta riskin merkittävyydestä ei voida vetää johtopäätöksiä.

Kyberriskit voivat vaikuttaa kyberturvallisuuteen aiheuttamalla onnettomuuksia, viivästymisiä, epäselviä tilanteita sekä luottamuksen menettämistä. Luvussa 2.1 käsitelty kyberriskien vahva keskeinen korrelaatio ja riskien mallintamisen vaikeus kuitenkin hankaloittavat vaikutusten arviointia. Kyberriskien toteutumisen todennäköisyys on kuitenkin maltillinen kautta aineiston, minkä vuoksi riskien merkittävyyden kyberturvallisuudelle voidaan todeta olevan tällä hetkellä maltillinen. Alhaisesta todennäköisyydestä huolimatta kyberriskeillä voi kuitenkin olla erittäin suuria haitallisia vaikutuksia toteutuessaan, minkä vuoksi on elintärkeää huomioida kyberriskit toimialan järjestelmäkehityksessä ja koulutuksessa.

Kyberriskien vaikutuksen siviili-ilmailun sääntelykehitykseen voidaan nähdä alkaneen vuodesta 2015, jolloin Euroopan komissio pyysi Euroopan ilmailustrategian välityksellä Euroopan lentoturvallisuusvirastoa tutkimaan kyberriskejä. Ilmailustrategia ehdotti myös uutta sääntelyä muun muassa kyberriskien huomioimiseksi. Uutta sääntelyä valmisteltiin kolme vuotta, jonka jälkeen uusi asetus 2018/1139 Euroopan yhteisistä siviili-ilmailun säännöistä säädettiin. Asetuksessa huomioitiin siviili-ilmailun kasvava riippuvuus nykyaikaisesta tieto- ja viestintäteknologiasta, vahvistaen kyberriskien vaikutusta uuden sääntelyn luomiseen.

Asetuksen lisäksi Euroopan lentoturvallisuusvirasto on tehnyt määräajoin päivitettäviä lentoturvallisuussuunnitelmia, joista voidaan havainnoida kyberriskin vaikutus. Vuosien 2014–2017 suunnitelma ei huomioinut kyberriskejä, mutta vuonna 2016 julkaistu suunnitelma otti huomioon kyberturvallisuuden osana uusia järjestelmiä. Huomioitavaa on myös se, että uusi suunnitelma päätettiin julkaista jo ennen vanhan päättymisajankohtaa. Vuonna 2016 julkaistu lentoturvallisuussuunnitelma toi myös esille kehitteillä olevan katselmuksen RMT.0648, jonka avulla pyrittiin tunnistamaan ja vähentämään ilmailualan kyberriskejä.

Siviili-ilmailuun keskittyvän sääntelyn lisäksi Euroopan unioni on reagoinut kyberriskeihin yleisen tietosuoja-asetus 2016/679:n, sekä verkko- ja tietojärjestelmien turvallisuusdirektiivi 2016/1148:n avulla. Yleinen tietosuoja-asetus keskittyi luonnollisten henkilöiden tietojen suojaamiseen määräämällä suostumuksesta, profiloinnista, yksilön oikeuksista, tietojenkäsittelijöiden velvoitteista, tietomurroista, kyberhyökkäyksistä ja rikesakoista. Lisäksi asetus määräsi tietosuojavastaavan asettamisesta yhtiöissä, joissa harjoitetaan laajamittaista tietojenkäsittelyä.

Turvallisuusdirektiivi 2016/1148 määräsi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi. Direktiivi velvoitti Euroopan unionin jäsenvaltioita tekemään kansallisen verkko- ja tietojärjestelmien turvallisuusstrategian ja nimeävän kyseisistä toimista vastuussa olevan viranomaisen. Direktiivi velvoittaa myös merkittävien turvallisuustapahtumien ilmoittamista viranomaisille ilmailualan osalta.

Myös toinen katselmus oli luotu kyberriskien sääntelyn edistämiseksi. Katselmus RMT.0720 on ollut kehitteillä vuodesta 2017 alkaen. Katselmus tähtää ilmailujärjestelmien suojaamiseen kyberhyökkäyksiltä ja niiden seuraamuksilta sääntelyjärjestelmän luomisella. Katselmuksen on arvioitu astuvan voimaan vuonna 2020, mikäli se hyväksytään.

Yleinen siviili-ilmailun asetus 2018/1139 astui voimaan syyskuussa 2018 määräten kyberturvallisuuden huomioimisesta lentoturvallisuussuunnitelman ja lentoturvallisuusohjelman laatimisessa. Lentoturvallisuussuunnitelman tehtävänä oli asettaa Euroopan ilmailutoiminnan turvallisuustaso. Jäsenvaltioilta vaadittiin laadittu lentoturvallisuusohjelma, jossa jäsenvaltiot kuvailevat turvallisuusriskien lieventämistoimia ja vahvistavat niiden vastuulla olevan ilmailutoiminnan hyväksyttävän turvallisuustason. Kyberriskien huomioiminen näkyy asetuksessa 2018/1139 myös vaadittuna yhteistyönä Euroopan lentoturvallisuusviraston ja jäsenvaltioiden välillä kyberturvallisuusasioissa. Lentoturvallisuusvirasto voi myös antaa jäsenmaille sitovia suosituksia kyberturvallisuutta korjaavista toimista.

Kyberriskien vaikutus sääntelykehitykseen on huomioitavissa myös valvonnan sääntelyssä. Asetuksessa 2018/1139 määrättiin riskipohjaisesta valvonnasta, joka koskee näin ollen myös kyberriskejä. Riskipohjaisesta valvonnasta ei kuitenkaan toistaiseksi ole tarvittavia ohjeita, minkä vuoksi sitä varten on julkaistu vasta suositeltuja käytäntöjä, joita ei voida käsittää sääntelyksi.

Asetusten, direktiivien ja tulevien katselmusten lisäksi ilmailualan järjestöt ovat julkaisseet suosituksia kyberriskistä johtuen. Suosituksia ei voida kuitenkaan pitää sääntelynä, minkä vuoksi ne eivät vastaa tutkimusongelmaan sellaisenaan vaan niistä voidaan vetää pelkkiä johtopäätöksiä toimialan sääntelyn tulevaisuuden suunnasta.

Sääntelyä on tehty Euroopan tasolla verrattain nopeasti kyberriskitietoisuuden lisääntyessä, mutta sääntelyn nopea kehitys on tehnyt sääntelyn tarkkuudesta ja implementoitavuudesta yleistä tasoa heikompaa. Luvussa 5.1 käsitelty katselmus RMT.0648 mainitsi suoraan, ettei kyberturvallisuutta ole huomioitu olemassa olevissa standardeissa, minkä vuoksi niitä joudutaan tällä hetkellä käsittelemään erityisehdon kautta. Erityisehto jättää kyberturvallisuuden huomioimisen vastuun sertifioivalle osapuolelle, joka voi aiheuttaa eroavaisuuksia sertifikaattien myönnössä.

Euroopan parlamentin ja komission tietosuoja-asetuksella 2016/679 määrättiin tietosuojavastaavan nimittäminen ja tietojen käsittelyn prosessit. Asetuksessa määrätään myös ilmoittamisvelvollisuudesta. Prosesseja valvotaan sakon uhalla, joka aiheuttaa myös siviili-ilmailun toimijoille pakon käyttää vaadittuja prosesseja. Vastaavia prosesseja ei kuitenkaan havaittu pelkästään kaupallisen siviili-ilmailun kyberriskiä käsittelevästä sääntelystä. Sääntely ei myöskään määrää toimijoiden kyberriskienhallintatoimenpiteistä siviili-ilmailussa. Esiin nostetut ongelmat sääntelyn laajuudesta, yleisluontoisuudesta ja prosesseista osoittavat, ettei sääntelyn osalta olla vielä täysin tietoisia miten kyberriskin tuomia uhkia voidaan säännellä.

Kaiken kaikkiaan kyberriskien voidaan nähdä kiihdyttäneen uuden sääntelyn määrää lähivuosina, mutta sääntelyn luotettavuus kärsii yleisluontoisuudesta ja eri direktiivien, asetusten ja suositeltujen käytäntöjen laajuus heikentää sääntelyn selkeyttä toimialan näkökulmasta katsottuna. Sääntelyn implementoinnin vaikeus voi heikentää sääntelyn turvallisuusvaikutuksia. Sääntelyn staattisuus voi myös heikentää sääntelyn turvallisuusvaikutuksia, sillä uutta sääntelyä tai sääntelyn korjauksia ei voida luoda määrättyä prosessia nopeammin.

6.2 Johtopäätökset

Tunnistettujen kyberuhkien määrä aineistossa oli suppea toimialan käyttämien teknologioiden määrään suhteutettuna, mikä viittaa siihen, ettei suurta osaa kyberuhkista ole vielä tunnistettu. Kyberuhkia ja kyberriskejä käsiteltiin pääosin melko yleisluontoisesti, eikä suuresta osasta uhkia ollut tunnistettu tai arvioitu niiden mahdollisia vaikutuksia tai todennäköisyyksiä. Tämän lisäksi tunnistetuista kyberuhkien vaikutuskohteista vain kaksi koskettivat kaikkia systemaattisen kirjallisuuskatsauksen aineistoja ja niitä koskevista uhkista oli havaittavissa erimielisyyksiä tutkimusten välillä. Tästä voidaan päätellä, ettei kyberriskien ja kyberturvallisuuden tekijöistä ole yhtenäistä kuvaa toimialan tutkimuksissa. Tutkimustiedon puutteesta voidaan myös vetää johtopäätös, ettei alalla välttämättä näin ollen ole tietoa sitä koskettavista kyberriskeistä. Yhtenäisen kuvan, riskien määrittelyn ja riskien tunnistamisen puuttuessa toimialan on vaikea ennakoida riskien vaikutusta. Tuntematonta riskiä on miltei mahdotonta hallita, mikä voi aiheuttaa toimialalle ongelmia niin tällä hetkellä, kuin tulevaisuudessa.

Aineiston yleinen konsensus oli, että kyberriskien merkitys siviili-ilmailulle tulee nousemaan tulevaisuudessa. Uudet järjestelmät, kuten ADS-B-järjestelmä, nähtiin aineistossa merkittävänä kyberriskin lähteenä. Luvussa 2.1 käsitellysti kyberriskit ovat myös hyvin dynaamisia, minkä vuoksi niiden kehittymisen voidaan nähdä olevan nopeaa. Uusien järjestelmien liittäminen pakolliseksi osaksi toimialan toimintaa ilman vankkaa kyberriskitietämystä ja nopeita turvallisuuspäivitysmahdollisuuksia voi näin ollen aiheuttaa perustavanlaatuisen ongelman toimialalle. Mikäli nopeita turvallisuuspäivityksiä ei oteta huomioon, saattaa alan toiminta keskeytyä pitkäksikin aikaa tuntemattoman tai heikosti tunnetun kyberriskin toteutuessa. Tapahtuma saattaa myös paljastaa alan tiedon puutteen kyberriskeistä. Tällaisen tapahtuman seurauksena voi olla merkittävä toimialan maineen ja luotettavuuden heikkeneminen. Luvussa 2.3 käsitellysti luotettavuus toimii osana kyberturvallisuutta, minkä vuoksi niin kutsuttua kybermaailmaa ei voida käyttää palveluiden tuottamiseen ilman luottamusta sen toimintaan. Luotettavuuden heikkeneminen voi siis aiheuttaa hyvin pitkäaikaisia vaikutuksia toimialalle niin toiminnan kehittämisen kuin kannattavuudenkin näkökulmasta.

Kyberriskejä ja kyberuhkia käsiteltiin toimialalla poikkeuksetta osana kyberturvallisuutta niin aineiston kuin sääntelijöidenkin toimesta. Kyberturvallisuuden tehtävänä on estää kyberriskien vaikutus turvallisuudelle tai minimoida toteutuneiden riskien vaikutusta. Riskienhallinnan

näkökulmasta katsottuna kyberturvallisuutta voitaisiin moittia yksiulotteiseksi, sillä se pyrkii vain poistamaan tai torjumaan riskiä. Tietoisuuden lisääntyessä riskienhallintametodit voivat lisääntyä ja fokus voi siirtyä kyberturvallisuudesta kyberriskien kokonaisvaltaiseen hallintaan, mutta aineistosta voidaan päätellä että näin ei ainakaan vielä ole tapahtunut. Yksinomaan kyberturvallisuuden näkökulman valitseminen voi altistaa alan erityisesti tuntemattomien kyberriskien vaikutuksille. Vaikutukset voivat olla suuremmat kun riskiä ei ole pyritty vakuuttamaan tai käsittelemään riskienhallinnan keinoin.

Sääntely on huomioinut kyberriskiä asetuksien ja direktiivien kautta, mutta myös sääntely keskittyy kyberturvallisuuteen ja jättää huomiotta kyberriskien vakuuttamisen tai kokonaisvaltaisen kyberriskien hallinnan. Euroopan komissio on pyytänyt ilmailustrategiassaan Euroopan lentoturvallisuusvirastoa tutkimaan kyberriskejä, mistä voidaan päätellä sääntelijöiden kyberriskituntemuksen olevan heikkoa. Kansainvälisen siviili-ilmailujärjestön päätöksestä A39-19 voidaan päätellä, ettei siviili-ilmailun järjestöjenkään kyberriskitietämys ole tällä hetkellä sääntelijöitä parempi.

Kyberriskit ovat uusia riskejä toimialalle, mikä näkyy myös aineistosta. Systemaattisen kirjallisuuskatsauksen aineistot ovat kehitetty vuosina 2016–2018, mikä osoittaa kyberriskitiedon nopeaa kehittymistä. Uusien yhteisten siviili-ilmailusääntöjen kehittämisessä meni noin kolme vuotta, jonka aikana kyberriskitietämys on myös edennyt merkittävästi. Tiedon lisääntyessä uutta sääntelyä ei kuitenkaan saada tehtyä nopeasti, sillä luvussa 3.4 käsitellysti uuden sääntelyn prosessi on kestoltaan pitkä ja monivaiheinen. Tiedon oletettava nopea kasvu sekä kyberriskien dynaamisuus vaatisivat myös dynaamista sääntelyä, joka osoittautuu nykyisellä sääntelyntekoprosessilla kuitenkin haastavaksi. Mikäli uusia direktiivejä ja asetuksia ei saada nopeasti voimaan, voi niiden vaikutus turvallisuudelle jäädä vähäiseksi riskien muuttuessa nopeasti.

Sääntelyn yleisluontoisuuden aiheuttamat sääntelyn tulkinnan haasteet kävivät myös ilmi käsitellystä aineistosta. Luvussa 3.2 käsitellysti hyvän sääntelyn edellytyksenä on yleisluontoisuus, jotta sääntely ei koske vain yksittäistapauksia. Luvussa käsitellysti liian yleisluontoinen sääntely aiheuttaa kuitenkin ongelman vallanjako-opin näkökulmasta, siirtäen valtaa sääntelystä tuomareille ja tulkintavirkamiehille. Valtioneuvosto mainitsi verkko- ja tietojärjestelmien turvallisuusdirektiivin vähimmäiskriteerien olevan epäselviä, joka tuo esiin sääntelyn tulkin-

nanvaraisuuden. Sääntelyn tulkinnanvaraisuus voi johtaa eri tulkintoihin Euroopan unionin jäsenmaiden ja toimialan toimijoiden välillä, mikä voi aiheuttaa eri turvallisuusvaatimuksia eri maissa. Luvun 2.1 mukaisesti kyberriski on globaalia, jolloin maantieteelliset rajat eivät vaikuta siihen. Mikäli vaatimukset ovat heikommat toisessa maassa, voi se aiheuttaa ongelmia myös sääntelyä tiukasti tulkitseville maille, heikentäen sääntelyn vaikutusta turvallisuuden ylläpitämiseen.

Maiden lisäksi toimialan toimijoiden eriasteinen sääntelyn tulkinta voi myös aiheuttaa turvallisuusongelmia, jotka vaikuttavat myös niihin, jotka ovat tulkinneet sääntöjä tiukemmin. Sääntelyn valvontaa on myös siirretty osittain jäsenvaltioille, jonka vuoksi heikosti tulkittua sääntelyä niin jäsenvaltioiden kuin toimialan toimijoiden osalta voi olla erittäin vaikea havaita valvonnan kautta. Kokonaisuudessaan ongelmat voivat aiheuttaa sääntelyn merkityksettömyyttä, ellei sääntely aseta selkeitä tavoitteita turvallisuudelle, kyberriskien torjunnalle, sääntelyn implementoinnille ja valvonnalle.

Sääntelyn kehittäminen kestää siis prosessien vuoksi kauan, mutta toisaalta uutta sääntelyä kyberriskien osalta on kehitetty lyhyessä ajassa melko paljon. Vuodesta 2016 eteenpäin on kehitetty verkko- ja tietojärjestelmädirektiivi, yleinen tietosuoja-asetus ja uudet yhteiset siviili-ilmailun säännöt. Näiden lisäksi kehitysvaiheessa on kaksi katselmusta, jotka voivat vaikuttaa siviili-ilmailun kyberriskien sääntelyyn lähitulevaisuudessa. Sääntelyn lisäksi luvussa 3.4 esitellyt järjestöt pyrkivät parantamaan toimialan kyberriskien huomioimista suositeltujen käytäntöjen ja standardien kautta. Järjestöt toimivat myös jäseniensä keskustelualustana sääntelyn sisällöstä, edesauttaen yhtenäistä tulkintaa ja nopeampia toimia kyberturvallisuuden vahvistamiseksi toimialalla.

Sääntelystä ja järjestöistä muodostuva kehikko on siviili-ilmailun toimijan näkökulmasta haastava, sillä pelkästään sääntelyn vaatimien toimien tulkinta ja implementointi voivat osoittautua hankaliksi. Standardit, suositellut käytännöt ja sääntely vaativat toimijoilta merkittävää aktiivisuutta. Järjestöt velvoittavat useissa tilanteissa jäseniään seuraamaan standardeja ja kehottavat seuraamaan myös suositeltuja käytäntöjä. Kansainvälisen siviili-ilmailujärjestön päätöksestä A39-19 voidaan lisäksi päätellä, että kyberriskien pohjalta tullaan tekemään järjestöjen standardeja ja suositeltuja käytäntöjä kun yhteisymmärrys kyberuhista, kyberriskeistä ja niiden vaikutuksista saadaan vakiinnutettua. Kehitysvaiheessa olevat katselmukset osoittavat myös mahdollisia muutoksia sääntelyyn tulevaisuudessa.

Toiminnan ohjeistuksen keskittymättömyys ja muutokset voivat näin ollen toimia tarkoitustaan vastaan, heikentäen sääntelyn ja standardien merkitystä turvallisuudelle. Luvussa 3.2 käsitellysti liian laaja sääntely tai sääntelyn jatkuva muuttuminen voi estää sääntelyn selvyyden ja selonoton, tehden sääntelystä oikeusturvan kannalta kestämätöntä. Sääntelyn muutostoimet ja järjestöjen standardi- ja käytäntökehitys voivat näin ollen lisätä epäselvyyttä heikentäen niin järjestöjen toimien kuin sääntelynkin vaikutusta turvallisuuteen, ellei niitä kehitetä maltillisesti ja toisiaan huomioiden.

Luvussa 5.1 esitelty katselmus RMT.0648 esitteli kyberturvallisuuden huomioimisen erityisehdon kautta. Erityisehto on tarkoituksella tehty laveaksi, jotta sitä voidaan käyttää sääntelemättömien uhkien torjuntaan. Erityisehdon pohjalta toimiminen kuitenkin heikentää sääntelyn luotettavuutta, sillä se siirtää vastuuta tulkitsevalle osapuolelle. Luvussa 5.1 tuotiin myös esille, ettei katselmus ollut edennyt käsittelyssä eteenpäin odotetussa aikataulussa, eikä siitä löytynyt tällä hetkellä mitään etenemistietoa Euroopan unionin sivustoilta. Sääntelyprosessin kankeus estää nopean käsittelyn, sillä kiireisetkin korjaukset käsitellään luvussa 3.4 esitellyn sääntelyn luomisprosessin kautta. Kaupallinen siviili-ilmailu on hyvin sääntelykeskeistä ja luottaa sääntelyn oikeellisuuteen turvallisuuden osalta. Erityisehto voi heikentää turvallisuutta ja asettaa siviili-ilmailun toimijoita eri asemaan, sillä erityisehdon tulkinta ei välttämättä ole aina tasalaatuista. Sääntelyn staattisuus heikentää sääntelyn mahdollisuuksia vastata dynaamisiin kyberriskeihin, joka voi edelleen heikentää toimialan turvallisuutta.

Kaiken kaikkiaan tutkielmassa tunnistettiin kyberriskien vakiintumattomuus toimialalla ja sääntelyssä. Uutena aiheena kyberriskit vaativat paljon tutkimusta ja analysointia, jotta niitä voidaan tunnistaa ja hallita. Toimialan kannalta tärkeänä voidaan pitää kyberriskin huomioimista kokonaisvaltaisena toiminnan riskinä pelkän turvallisuusasian sijaan. Sääntelijöiden kannalta erityiseen keskiöön nousee selkeän, keskittyneen, kattavan ja helposti implementoitavan sääntelyn luominen, jotta sääntelyn tehokkuus varmistetaan.

6.3 Tutkielman arviointi

Tutkielman arvioinnin tehtävänä on arvioida tutkielman reliaabeliutta ja merkittävyyttä kriittisesti. Reliaabeliudella tarkoitetaan tutkielman kykyä antaa ei-sattumanvaraisia tuloksia

(Hirsjärvi ym. 2009, 231). Aiheen merkittävyyden tarkastelu keskittyy tutkimaan sitä, onko aiheella merkitystä tieteellisen tutkimuksen näkökulmasta. Aiheena kyberriskit siviili-ilmailussa ovat hyvin uusia ja niitä on tutkittu hyvin vähän valitusta näkökulmasta. Kokoavia tutkimuksia ei ole tehty, jonka vuoksi tutkimusmenetelmä valittiin.

Aiheen pääasiallinen merkittävyys on sen uutuudessa, minkä vuoksi tutkielman tehtävänä on esitellä ja yhtenäistää tutkimustuloksia sekä nostaa esiin havaintoja, joiden pohjalta voidaan tehdä uutta tutkimusta. Tutkielma vastaa valittuihin tutkimusongelmiin liittäen aineistosta synteesillä löydetyt kyberuhat ja kyberriskit operationaalisten kyberriskien kehikkoon, luoden yhtenäisyyttä tutkittavalle aiheelle ja antaen sille yhdistävää teoreettista pohjaa. Synteesillä verrataan tämän hetken tutkimustuloksia merkittävistä riskeistä, esitellen niiden erimielisyyksiä ja yhtenäisyyksiä. Sääntelyn osalta tutkielma kokoaa merkittävän tiedon ja tuo siitä esille mahdollisia heikkouksia hyvän sääntelyn teoriaan verraten. Operationaalisten riskien teoriaa ei ole aiemmin liitetty siviili-ilmailun kyberriskin tutkimuksiin. Erimielisyyksiä ei ole myöskään esitelty aiemmissa tutkimuksissa. Euroopan siviili-ilmailun osalta tietoa ei tiettävästi ole kerätty tutkimukseen. Näiden tuominen tutkielmaan lisää aiheen merkittävyyttä. Vastaukset eivät kuitenkaan ole täysin tyhjentäviä, minkä vuoksi ne voidaan nähdä aiheen näkökulmia esittelevänä ja jatkotutkimuksia kannustavana tiedon syventämiseksi entisestään.

Tutkielman systemaattiseen kirjallisuuskatsaukseen valitusta aineistosta voidaan löytää kriittisesti tarkasteltavia kohtia. Systemaattisessa kirjallisuuskatsauksessa keskiössä on valintaprosessi, joka tutkielmassa onnistuttiin tekemään tiukoilla kriteereillä löytäen aiheelle merkityksellistä aineistoa. Tiukat kriteerit ja rajallinen tutkimusmäärä aiheesta rajasivat valitut tutkimukset niukkaan joukkoon. Valittu joukko on kuitenkin systemaattisen kirjallisuuskatsauksen teoriaa noudattava, sillä tiukkojen kriteerien vuoksi systemaattinen kirjallisuuskatsaus voi olla aineistoltaan muita kirjalisuuskatsauksia pienempi (Petticrew 2001, 99). Tiukoilla valintakriteereillä ja valinnan huolellisella esittelyllä varmistetaan tutkielman reliaabelius.

Määritettyyn kysymykseen vastaamisen ja tiukkojen kriteerien lisäksi systemaattiselle kirjallisuuskatsaukselle on tärkeää objektiivisen yhteenvedon tekeminen ja aineiston laadun arviointi (Petticrew 2001, 99). Tutkielmassa objektiivinen yhteenveto saavutettiin noudattamalla erityistä huolellisuutta aineistoon viitatessa ja lähdeviittausten merkinnöissä. Viittauksissa ei

tuotu esiin mielipiteitä tai havaintoja, vaan havainnot eriytettiin viittauksista selkeillä huomautuksilla.

Valitun aineiston laadun tarkastelusta voidaan nostaa esiin kriittisiä huomioita. Haassin ym. (2016) tutkimus sekä Kesslerin & Craigerin (2018) tieteellinen konferenssiesitelmä on julkaistu Embry-Riddle Aeronautical Universityn toimesta. Haassin ym. (2016) tutkimus käsittelee kuitenkin siviili-ilmailua ja kyberturvallisuutta esittelevältä kannalta, jonka vuoksi se ei pureudu syvälle kyberuhkiin ja kyberriskeihin. Julkaisun tarkoituksena on pääosin tuoda esille mahdollisia vaikutuskohteita ja kannustaa tutkijoita tutkimaan aihetta lisää. Julkaisun yleisluontoisuus kavensi analyysin vertailun laajuutta. Julkaisussa ei myöskään listata lähteitä kerätylle tiedolle. Julkaisun luotettavuutta lisää kuitenkin sen julkaisu alalla erittäin tunnetun yliopiston toimesta. Julkaisun kirjoittajista Haass on Massachusetts Institute of Technologystä tohtoriksi väitellyt, Embry-Riddle Aeronautical Universityn Arizonan kampuksen dekaani (ERAU 2018a) ja Sampigethaya on Washingtonin yliopistosta tohtoriksi väitellyt, samalla kampuksella toimiva apulaisprofessori (ERAU 2018b). Julkaisun kolmas kirjoittaja Capezzuto on Aireon nimisen yrityksen teknologiajohtaja (Aireon 2018). Erityisesti Haassin ja Sampigethayan akateemiset taustat lisäävät julkaisun luotettavuutta.

Kessler ja Craiger toimivat myös Embry-Riddle Aeronautical Universityssä. Kessler on väitellyt tohtoriksi Novan yliopistosta Miamissa ja toimii Embry-Riddlen yliopiston kyberturvallisuuden osaston professorina (ERAU 2018c). Craiger on väitellyt tohtoriksi University of South Floridasta ja toimii Embry-Riddlen yliopiston apulaisprofessorina turvallisuustutkimusten osastolla (ERAU 2018d). Kesslerin & Craigerin (2018) tieteellinen konferenssiesitelmä ei kuitenkaan listaa kaikkia käyttämiään lähteitä ja käsittelee tieteellisen konferenssiesitelmän muodossa tietoa todella kompaktissa muodossa. Tämä vaikeuttaa julkaisun objektiivista referointia, minkä vuoksi tutkielmassa käytettiin ADS-B-järjestelmän osalta julkaisun käyttämää lähdettä. Lähteen käyttäminen helpotti objektiivista viittaamista.

Standerin & Ophoffin (2016) tutkimus on julkaistu Imam Journal of Applied Sciencesissä. Kriittisenä huomiona voidaan esittää Imam Journal of Applied Sciencesin tuntemattomuus. Journaalin luotettavuutta lisää sen vertaisarviointi, sekä sen rekisteröityneisyys tunnettuihin palveluihin, kuten Google Scholariin, EBSCO Publishingiin, Ex-Librikseen ja ProQuestiin (IJAS

2018). Stander ja Ophoff toimivat luennoitsijoina University of Cape Townin informaatioteknologian osastolla (UCT 2018). Tekijöiden akateeminen tausta ja journaalin esittelemät luottamustekijät antavat julkaisulle luotettavuutta. Julkaisun pääfokuksena on osoittaa, ettei kyberhyökkäys lentokoneen järjestelmiin ole mahdottomuus. Tämän vuoksi julkaisu käsittelee kyberriskiä ja kyberuhkia vain lentokoneeseen vaikuttavan teknologian osalta. Julkaisu ei myöskään esittele uhkia syvällisesti, eikä se tuo niiden todennäköisyyttä tai vaikutusta esille merkittävissä määrin. Tutkielmassa pystyttiin tunnistamaan alalle merkittäviä riskejä synteesin avulla ja analysoimaan mainittuja uhkien osa-alueita, mutta riskien ja uhkien pintapuolinen käsittely julkaisussa kavensi synteesin tunnistamia yhteisiä riskejä ja uhkia, sekä analyysin vertailun laajuutta.

Strohmeierin ym. (2017) tutkimus on julkaistu tekniikan alan järjestö IEEE:n journaalissa. IEEE:tä pidetään yleisesti luotettavana järjestönä ja journaali julkaisee sivuillaan merkittävän määrän luotettavuustietoja (IEEE 2018). Tutkimus on julkaistu myös Oxfordin yliopiston sivuilla, joka lisää julkaisun luotettavuutta (University of Oxford 2017). Tutkimus tutkii langattomien teknologioiden vaikutusta kyberturvallisuuteen, jonka vuoksi se rajaa tutkimuksesta kaikki muut teknologiat pois. Aineistoa tarkastellessa kävi ilmi, että muutkin tutkimukset keskittyivät vahvasti langattomien teknologioiden kyberuhkiin ja -riskeihin, mutta mahdolliset muut huomiot olisivat voineet laajentaa synteesin esiin tuomia uhkia ja riskejä, sekä analyysin vertailun laajuutta.

Sääntelyn osalta Euroopan unionin lakikirjasto toimi päälähteenä kirjallisuuskatsaukselle, jonka vuoksi aineiston luotettavuutta voidaan pitää hyvänä. Aineiston keruun prosessia ei kuitenkaan voitu kuvailla yhtä tarkasti kuin systemaattisen kirjallisuuskatsauksen osiossa, sillä lakikokoelma ei automaattisesti listaa yhteen toimialaan tai sen osa-alueeseen vaikuttavia asetuksia ja direktiivejä. Tämä heikentää tutkielman toistettavuutta. Toistettavuuden mahdollistamiseksi hakuprosessista kuvailtiin kuitenkin hakutermien käyttö ja aineiston keruun pääprosessit, mikä mahdollistaa tutkielman toistettavuuden. Järjestöjen valinta perusteltiin merkittävyydellä ja valitut järjestöt tarkistettiin luotettavuuden osalta. Järjestöjä on kuitenkin todella monia, minkä vuoksi järjestövalinnan voisi tehdä myös toisella tavalla jatkotutkimuksissa. Tämän vuoksi järjestöjen valintaperusteet esiteltiin huolellisesti.

Kaiken kaikkiaan tutkielman systemaattiseen kirjallisuuskatsaukseen valittua aineistoa voidaan pitää luotettavana, mutta aineiston laajuus voitiin nähdä kohtuullisen suppeana. Synteesissä tuotiin kuitenkin esiin aineiston suppeus tunnistettujen kyberuhkien ja -riskien osalta ja analyysillä pystyttiin tuomaan esiin havaintoja aineistosta, minkä vuoksi aineistoa ei voida pitää liian suppeana tutkielman tekemistä varten. Aineiston tunnistamien uhkien ja riskien suppeus osoittaa aiheen uutuuden ja tutkimuksen lisätarpeen aiheesta, joka voidaan nähdä tutkielman ansioksi. Tutkielma onnistui aineiston suppeudesta huolimatta antamaan kuvan tällä hetkellä tunnistetuista kyberuhkista ja -riskeistä ja analysoimaan niitä merkittävällä tavalla.

Sääntelyn kirjallisuuskatsausta voidaan pitää luotettavana valitun päälähteen, järjestöjen valinnan perustelun ja hakuprosessin kuvaamisen vuoksi. Luvuissa 4 ja 5 esitellyt havainnot erotettiin selvästi tutkielman aineiston viittauksista, mikä tuo tutkielmalle objektiivisuutta ja auttaa lukijaa erottamaan tutkijan omat havainnot lähteiden sisällöstä.

6.4 Lopuksi

Tutkielma esitteli kyberriskien vaikutusta Euroopan siviili-ilmailun kyberturvallisuuteen ja sääntelyyn kirjallisuuskatsauksen menetelmällä. Tutkielmassa huomattiin, ettei siviili-ilmailun kyberriskejä ole laajalti liitetty aiemmin kehitettyyn kyberriskin teoriaan, eikä niistä näin ollen ole yhtenäistä kuvaa toimialan tutkimuksissa. Syvempää tutkimusta voitaisiin tehdä järjestelmäperusteisesti, jolloin siviili-ilmailun järjestelmien kyberuhkista saataisiin luotua kokonaisvaltaisempia arvioita ja niistä voitaisiin muodostaa riskienhallinnan teoriaan vahvemmin nojaavaa tutkimusta. Kyberriskejä on tällä hetkellä käsitelty kyberturvallisuuden näkökulmasta, mutta riskienhallinnan näkökulmasta tutkimusta puuttuu niin kyberriskien luokittelun kuin todennäköisyyksien ja vaikutusten arvioinninkin osalta. Siviili-ilmailun kyberriskien tutkimustiedon ja vaikutusten arvioinnin kehittyessä myös vakuuttamisen mahdollisuutta olisi aiheellista tutkia. Riskienhallinnan näkökulma tarjoaakin näin ollen paljon mahdollisia uusia jatkotutkimuskohteita aiheen pohjalta. Toimialan näkökulman sijaan myös siviili-ilmailun vakuuttajien ja jälleenvakuuttajien näkökulmaa voitaisiin tarkastella kyberriskin puitteissa. Vakuuttajien ja jälleenvakuuttajien kyberriskien huomioiminen ja tuotekehitys siviili-ilmailulle tarjoaa näin ollen mahdollisia jatkotutkimuskohteita.

Tutkimustietoa on kyberriskeistä siviili-ilmailussa tehty erityisesti lähivuosina merkittävän paljon, minkä vuoksi voidaan olettaa tutkimustiedon lisääntyvän lähitulevaisuudessakin merkittävästi. Toimialan ymmärryksen lisääntyessä uusi kirjallisuuskatsaus kyberriskien havainnoinnista toimialalla voisi tuoda mielenkiintoisen tarkastelukulman, sillä sitä voitaisiin verrata aikaisempiin kirjallisuuskatsauksiin. Kirjallisuuskatsauksella voitaisiin tutkia tiedon lisääntymisen kehityskulkua, sekä tiedon lisääntymisen vaikutusta riskienhallintatoimiin siviili-ilmailun toimijoiden osalta.

Sääntelyn puolesta Euroopan unionissa ja järjestöissä tapahtuvat uudet aloitteet ja niiden mahdollisen hyväksymiset, korjaukset ja hylkäämiset tulevaisuudessa tarjoavat jatkotutkimuskohteita, joilla on selvä merkitys alan toiminnalle. Eurooppalaisen sääntelyn osalta olisi aiheellista tutkia myös sääntelyn vaikutuksia Euroopan siviili-ilmailun toimijoiden kilpailukyvylle. Sääntelyn implementoinnin maakohtaiset eroavaisuudet voivat tarjota jatkotutkimuskohteita, mikäli eroavaisuuksia löydetään Euroopan unionin jäsenmaiden välillä. Tutkielmassa muodostetun käsityksen mukaan eroavaisuuksia voidaan lähitulevaisuudessa olettaa löytyvän, jonka vuoksi asiasta olisi hyödyllistä saada myös tutkimustietoa.

LÄHDELUETTELO

Kirjallisuus:

Baldwin, R. Cave, M. & Lodge, M. 2011. Understanding Regulation: Theory, Strategy, and Practice. Oxford University Press USA - OSO, Oxford.

Bandyopadhyay, T. Mookerjee, V. & Rao R. 2009. Why IT Managers Don't Go for Cyber Insurance Products. Communications of the ACM. Kennesaw State University.

Banta, Victor. 2012. The Strategic Management of Risk, Threats and Vulnerabilities, in an Informational System. Valahian Journal of Economic Studies. Vol. 3. No. 1. pp. 7–16.

Baumeister, Roy F. & Leary, Mark R. 1997. Writing Narrative Literature Reviews. Review of General Psychology. Vol 1. No. 3. pp. 311–320.

Biener, Christian. Eling, Martin. & Wirfs, Jan. 2015. Insurability of Cyber Risk: An Empirical Analysis. Palgrave Macmillan UK. The Geneva Papers on Risk and Insurance – Issues and Practice. Vol. 40. 131–158.

Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University.

Cruz-Cunha, Maria. Portela, Irene. 2015. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. Hershey, PA: IGI Global.

De Cerchio, R. Riley, C. 2011. Aircraft Systems Cyber Security. 30th Digital Avionics Systems Conference.

EASA. 2014. European Aviation Safety Plan 2014-2017. Saatavilla: https://www.caa.md/files/2014_01/581.pdf (Viitattu 13.11.2018)

EASA. 2016a. European Aviation Safety Plan 2016–2020. Saatavilla: https://www.easa.europa.eu/sites/default/files/dfu/EPAS%202016-2020%20FINAL.PDF (Viitattu 13.11.2018)

EASA. 2016b. Launch of Rulemaking Task RMT.0648 "Aircraft Cybersecurity". Saatavilla: https://www.easa.europa.eu/newsroom-and-events/news/launch-rulemaking-task-rmt0648-%E2%80%9Caircraft-cybersecurity%E2%80%9D (Viitattu 14.11.2018)

EASA. 2016c. Aircraft cybersecurity. RMT.0648 – Issue 1 – 17.5.2016. Saatavilla: https://www.easa.europa.eu/sites/default/files/dfu/ToR%20RMT.0648%20Issue%201.pdf (Viitattu 14.11.2018)

EASA. 2016d. Practices for risk-based oversight. Saatavilla: https://www.easa.europa.eu/sites/default/files/dfu/RBO%20paper%2020161122_final.pdf (Viitattu 16.11.2018)

EASA. 2017. The European Plan for Aviation Safety (EPAS) 2018–2022. Saatavilla: https://www.easa.europa.eu/sites/default/files/dfu/EPAS_2018-2022%20v2.2.8%20for%20MB.pdf (Viitattu 13.11.2018)

Eling, Martin. & Schnell, Werner. 2016. What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. Vol. 17. No. 5. 474–491.

ENISA. 2017. ENISA Threat Landscape Report 2017. European Agency for Network and Information Security. Saatavilla: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (Viitattu 16.11.2018)

Euroopan komissio. 2015a. Euroopan lentoturvallisuusohjelmaa käsittelevän asiakirjan toinen versio. Saatavilla: https://eur-lex.europa.eu/resource.html?uri=cellar:f0a0e4cd-9ce8-11e5-8781-01aa75ed71a1.0007.02/DOC_2&format=PDF (Viitattu 18.10.2018)

Euroopan komissio. 2015b. An Aviation Strategy for Europe. Saatavilla: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0598 (Viitattu 6.11.2018)

FAA. 2008. Special conditions: Boeing model 787 8 airplane; systems and data networks security – Isolation or protection from unauthorized passenger domain systems access. Washington: Government Printer.

Fahey, E. 2014. EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation. Vol. 5. No. 1. pp. 46–60.

Fink, Arlene. 2005. Conducting research literature reviews: From the Internet to paper. 2. painos. Thousand Oaks: Sage.

Haass, Jon. Sampigethaya, Radhakrishna. & Capezzuto, Vincent. 2016. Embry-Riddle Aeronautical Univesity. Aviation and Cybersecurity: Opportunities for Applied Research. 39–43.

Hampton, John J. 2015. Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity. 2. painos. New York: AMACOM.

Hirsjärvi, Sirkka. Remes, Pirkko & Sajavaara, Paula. 2009. Tutki ja kirjoita. 15. uudistettu painos. Hämeenlinna. Kariston Kirjapaino Oy.

IATA. 2015. Position Paper on Cybersecurity. IATA. Saatavilla: https://www.iata.org/policy/Documents/cyber-threat-position.pdf (Viitattu 05.11.2018)

ICAO. 2011. Annex 17 to the Convention on International Civil Aviation. Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference. ICAO. Saatavilla: http://code7700.com/pdfs/icao_annex_17_9th_edition_march_2011_.pdf (Viitattu 28.11.2018)

ICAO. 2016. Addressing Cybersecurity In Civil Aviation. Assembly – 39th Session. Working Paper. ICAO. Saatavilla: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_en.pdf (Viitattu 24.10.2018)

ICAO. 2018d. Considerations About Cybersecurity. ICAO. Saatavilla: https://www.icao.int/Meetings/anconf13/Documents/WP/wp_160_en.pdf (Viitattu 22.10.2018)

Institute of Risk Management. 2014. Cyber Risk Executive Summary. The Institute of Risk Management. Saatavilla: https://www.theirm.org/media/2293893/IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf (Viitattu 22.8.2018)

ISO. 2018. ISO/IEC 27005:2018. International Organization for Standardization. Saatavilla: https://www.iso.org/standard/75281.html

Juul, Maria. 2016. New civil aviation safety rules. Briefing. EU Legislation in Progress. EPRS European Parliamentary Research Service. Euroopan parlamentti. Saatavilla: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573933/EPRS_BRI(2016)573933_EN.pdf

Kacem, T. Wijesekera, D. Costa, P. Carvalho, J. Monteiro, M. & Barreto, A. 2015. Key distribution mechanism in secure ADS-B networks. Conference Paper: Integrated Comm. Navigation and Surveillance (ICNS).

Kessler, Gary C. & Craiger. J. Philip. 2018. Aviation Cybersecurity: An Overview. National Training Aircraft Symposium (NTAS). 37. Embry-Riddle Aeronautical University.

Leonardi, M. Piracci, E. & Galati, G. 2014. ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. IEEE Tyrrhenian International Workshop on Digital Communications Enhanced Surveillance of Aircraft and Vehicles.

Limnéll, Jarmo. Majewski, Klaus. & Salminen, Mirva. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Petticrew, Mark. 2001. Systematic Reviews from Astronomy to Zoology: Myths and Misconceptions. British Medical Journal. Vol. 322. No. 7278. pp. 98–101.

PricewaterhouseCoopers. 2016. Aviation perspectives - 2016 special report series: Cybersecurity and the airline industry. Saatavilla: https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity.pdf (Viitattu 12.9.2018)

Purton, Leon. Abbass, Hussein. & Alam, Sameer. 2010. Identification of ADS-B System Vulnerabilities and Threats. Australasian Transport Research Forum 2010 Proceedings. Defence and Security Applications Research Centre. University of New South Wales. Australia.

Salminen, Ari. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja.

Selznick, P. 1985 Focusing Organisational Research on Regulation. Regulatory Policy and the Social Sciences. University of California Press, Berkeley.

Stander, Adrie. & Ophoff, Jacques. 2016. Cyber security in civil aviation. Imam Journal of Applied Sciences. 2016. Vol. 1. Iss. 1. pp. 23-26.

Strohmeier, Martin. Schäfer, Matthias. Pinheiro, Rui. Lenders, Vincent. & Martinovic, Ivan. 2017. IEEE Transactions on Intelligent Transportation Systems. Vol. 18. No. 6. pp. 1338-1357.

Tuomi, Jouni & Sarajärvi, Anneli. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki. Tammi.

Ulsch, N. MacDonnell. 2014. Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks. 1. painos. Hoboken, New Jersey: Wiley.

Urban, Jennifer A. 2017. Not Your Grandaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices Within the International Aviation Industry. 27 Albany Law Journal of Science and Tehcnology. Vol 27. No. 2. pp. 62–93.

Uusitalo, Hannu. 2001. Tiede, tutkimus ja tutkielma. Helsinki: Sanoma Pro Oy.

Valtioneuvosto. 2017. Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. Valtioneuvoston julkaisut.

Wuolijoki, Sakari. 2016. Hyvän sääntelyn periaatteet ja finanssialan viimeaikainen sääntely. Vakuutus- ja rahoitusneuvonta 45 vuotta. FINE. Vakuutus- ja rahoitusneuvonta, Helsinki. Saatavilla: https://www.fine.fi/media/julkaisut-2017/sakari-wuolijoki-hyvan-saantelyn-periaatteet-ja-finanssialan-viimeaikainen-saantely.pdf (Viitattu 18.10.2018)

Young, D. Lopez Jr., J. Rice, M. Ramsey, B. & McTasney, R. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection. Vol. 14. pp. 43–57.

Internet-lähteet:

Aireon. View All Management Team. Vincent Capezzuto. Saatavilla: https://aireon.com/company/management/vincent-capezzuto/ (Viitattu 6.12.2018)

Delta. 2018. Delta Airlines: Our Business: UPDATED: Statement on [24]7.ai cyber incident. Saatavilla: https://news.delta.com/updated-statement-247ai-cyber-incident (Viitattu 22.9.2018)

Department of Justice. 2017. Notice of Security Incident – New Hampshire. Saatavilla: https://www.doj.nh.gov/consumer/security-breaches/documents/virgin-america-20170726.pdf (Viitattu 24.9.2018)

EASA. 2018a. Cybersecurity Overview. EASA. Saatavilla: https://www.easa.europa.eu/easa-and-you/cyber-security/overview (Viitattu 20.11.2018)

EASA. 2018b. The Agency – About EASA. Saatavilla: https://www.easa.europa.eu/the-agency/faqs/agency#category-about-easa (Viitattu 1.10.2018)

EASA. 2018c. Cooperation with the International Civil Aviation Organisation (ICAO). Saatavilla: https://www.easa.europa.eu/easa-and-you/international-cooperation/cooperation-with-ICAO (Viitattu 24.10.2018)

ECAC. 2018a. About ECAC. Saatavilla: https://www.ecac-ceac.org/about-ecac (Viitattu 13.10.2018)

ECAC. 2018b. ECAC Member States. Saatavilla: https://www.ecac-ceac.org/member-states (Viitattu 13.10.2018)

ECAC. 2018c. ECAC Resolutions and Recommendations. Saatavilla: https://www.ecac-ceac.org/resolutions-and-recommendations (Viitattu 15.10.2018)

ENISA. 2016. Securing Smart Airports. Saatavilla: https://www.enisa.europa.eu/publications/securing-smart-airports/at_download/fullReport (Viitattu 7.11.2018)

ERA. 2018. GDPR: The impact for airlines. Saatavilla: https://www.eraa.org/system/files/ri_janfeb_gdpr_p16.pdf (Viitattu 12.11.2018)

ERAU. 2018a. Faculty at Embry-Riddle. Profile: Jon Haass. Saatavilla: https://faculty.erau.edu/Jon.Haass (Viitattu 6.12.2018)

ERAU. 2018b. Faculty at Embry-Riddle. Profile: Radhakrishna Sampigethaya. Saatavilla: http://faculty.erau.edu/Radhakrishna.Sampigethaya (Viitattu 6.12.2018)

ERAU. 2018c. Faculty at Embry-Riddle. Profile: Gary C. Kessler. Saatavilla: https://faculty.erau.edu/Gary.Kessler (Viitattu 6.12.2018)

ERAU. 2018d. Faculty at Emrby-Riddle. Profile: John Philip Craiger. Saatavilla: https://faculty.erau.edu/John.Craiger (Viitattu 6.12.2018)

EUROCONTROL. 2018a. Who We Are. Saatavilla: https://www.eurocontrol.int/articles/who-we-are (Viitattu 18.10.2018)

EUROCONTROL. 2018b. Our Role. Saatavilla: https://www.eurocontrol.int/articles/our-role (Viitattu 19.10.2018)

Euroopan komissio. 2018a. Aviation Security. Saatavilla: https://ec.europa.eu/transport/modes/air/security_en (Viitattu 12.10.2018)

Euroopan komissio. 2018b. Aviation Safety Policy in Europe. Saatavilla: https://ec.europa.eu/transport/modes/air/safety_en (Viitattu 18.10.2018)

Euroopan komissio. 2018c. European Aviation Safety Rules. Saatavilla: https://ec.europa.eu/transport/modes/air/safety/safety-rules_en (Viitattu 8.11.2018)

Euroopan parlamentti. 2018. Aviation safety. European parliament. Saatavilla: http://www.europarl.europa.eu/factsheets/en/sheet/134/aviation-safety (Viitattu 2.10.2018)

Euroopan unioni. 2018a. Euroopan komissio – Perustiedot. Saatavilla: https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_fi (Viitattu 15.10.2018)

Euroopan unioni. 2018b. Euroopan lentoturvallisuusvirasto (EASA) – Perustiedot. Saatavilla: https://europa.eu/european-union/about-eu/agencies/easa_fi (Viitattu 16.10.2018)

Eurooppa-neuvosto. 2018a. Vaihe 1: Säädösehdotus. Saatavilla: http://www.consilium.europa.eu/fi/council-eu/decision-making/ordinary-legislative-procedure/legislative-proposal/ (Viitattu 19.9.2018)

Eurooppa-neuvosto. 2018b. Vaihe 2: Ensimmäinen käsittely. Saatavilla: http://www.consilium.europa.eu/fi/council-eu/decision-making/ordinary-legislative-procedure/first-reading/ (Viitattu 19.9.2018)

Eurooppa-neuvosto. 2018c. Vaihe 3: Toinen käsittely. Saatavilla: http://www.consilium.europa.eu/fi/council-eu/decision-making/ordinary-legislative-procedure/second-reading/ (Viitattu 19.9.2018)

Eurooppa-neuvosto. 2018d. Vaihe 4: Sovittelu. Saatavilla: http://www.consilium.europa.eu/fi/council-eu/decision-making/ordinary-legislative-procedure/conciliation/ (Viitattu 19.9.2018)

Eurooppa-neuvosto. 2018e. Vaihe 5: Kolmas käsittely. Saatavilla: http://www.consilium.europa.eu/fi/council-eu/decision-making/ordinary-legislative-procedure/third-reading/ (Viitattu 19.9.2018)

FAA. 2012. Frequently asked questions – European Aviaation Safety Agensy (EASA). Saatavilla: https://www.faa.gov/aircraft/air_cert/international/easa/media/EASA_FAQ.pdf (Viitattu 28.10.2018)

IAOPA. 2018. What is General Aviation. Definition. IAOPA Europe. Saatavilla: https://www.iaopa.eu/what-is-general-aviation (Viitattu 13.12.2018)

IATA. 2018a. About Us. Saatavilla: https://www.iata.org/about/pages/index.aspx (Viitattu 28.9.2018)

IATA. 2018b. Vision and Mission. Saatavilla: https://www.iata.org/about/Pages/mission.aspx (Viitattu 28.9.2018)

IATA. 2018c. IATA's Industry Priorities and Targets. Saatavilla: https://www.iata.org/about/Pages/priorities.aspx (Viitattu 28.9.2018)

ICAO. 2018a. Civil Aviation Cybersecurity Information Repository. Saatavilla: https://www.icao.int/cybersecurity/Pages/default.aspx (Viitattu 22.10.2018)

ICAO. 2018b. About ICAO. Saatavilla: https://www.icao.int/about-icao/Pages/default.aspx (Viitattu 15.10.2018)

ICAO. 2018c. Frequently Asked Questions. Saatavilla: https://www.icao.int/about-icao/FAQ/Pages/icao-frequently-asked-questions-faq-14.aspx (Viitattu 15.10.2018)

IEEE. 2018. IEEE Transactions on Intelligent Transportation Systems. About Journal. Saatavilla: https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=6979 (Viitattu 6.12.2018)

IJAS. 2018. Imam Journal of Applied Sciences. About us. Saatavilla: http://www.e-ijas.org/aboutus.asp (Viitattu 6.12.2018)

JAATO. 2018a. Background. Saatavilla: https://jaato.com/page/101/ (Viitattu 28.9.2018)

JAATO. 2018b. New Basic Regulation (EU) 2018/1139 - Introduction Course. Saatavilla: https://jaato.com/courses/691/pdf/ (Viitattu 12.11.2018)

Trafi. 2018a. Säädökset. Saatavilla: https://www.trafi.fi/ilmailu/saadokset (Viitattu 12.10.2018)

Trafi. 2018b. EU-Säädökset. Saatavilla: https://www.trafi.fi/ilmailu/saadokset/eu-saadokset (Viitattu 12.10.2018)

Trafi. 2018c. Kansainväliset sopimukset. Saatavilla: https://www.trafi.fi/ilmailu/saadokset/kansainvaliset_sopimukset (Viitattu 13.10.2018)

Trafi. 2018d. Ilmoitus kauko-ohjatun ilma-aluksen käyttämisestä. Saatavilla: https://www.trafi.fi/ilmailu/miehittamaton_ilmailu/kauko-ohjatun_ilma-aluksen_kaytosta_ilmoittaminen (Viitattu 13.10.2018)

UCT 2018. University of Cape Town. Faculty of Commerce. Saatavilla: https://www.commerce.uct.ac.za/InformationSystems/People (Viitattu 6.12.2018)

University of Oxford. 2017. Research: On Perception and Reality in Wireless Air Traffic Communication Security. Saatavilla: https://www.cs.ox.ac.uk/publications/publication10662-abstract.html (Viitattu 20.11.2018)

Oikeudelliset lähteet:

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

Euroopan parlamentin ja neuvoston asetus (EU) 2018/1139 yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan unionin lentoturvallisuusviraston perustamisesta, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 2111/2005, (EY) N:o 1008/2008, (EU) N:o 996/2010, (EU) N:o 376/2014 ja direktiivien 2014/30/EU ja 2014/53/EU muuttamisesta sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 552/2004, (EY) N:o 216/2008 ja neuvoston asetuksen (ETY) N:o 3922/91 kumoamisesta.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa

Kansainvälisen siviili-ilmailun yleissopimus 11/1949

Komission täytäntöönpanoasetus (EU) N:o 646/2012 sakkoja ja uhkasakkoja koskevista yksityiskohtaisista säännöistä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 mukaisesti

Ilmailulaki (7.11.2014/864)